Počítačová kriminalita a minimalizace ztrát v oblasti informačních technologií

Computer crime and minimization of losses in information technology

bc. Ondřej ŠEDA

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Ondřej ŠEDA**
Osobní číslo:	**A08811**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Počítačová kriminalita a minimalizace ztrát v oblasti informačních technologií**

Zásady pro vypracování:

1. **Zjistěte k jakému zcizování nejčastěji dochází.**
2. **Zjistěte, zda se firmy zcizování brání a jak.**
3. **Zjistěte jaký je postih a zda firmy trvají na postihu při menších krádežích.**
4. **Zpracujte několik metod zjišťování, zda ke zcizení došlo či nikoliv.**
5. **Doporučte postup / řešení jak minimalizovat ztráty.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JÜTTNER, Alfred. O kriminologii a kriminalitě. 1. vyd. Praha : Orbis, 1968. 214 s. Zákony II/2009 : sborník úplných znění zákonů obchodního, občanského a trestního práva a souvisejících předpisů platných k 1.1.2009. Český Těšín : Poradce, 2009. 848 s.**
2. **DIEM, Walter. Bezpečnostní zařízení. Praha : Ikar, 2000. 110 s. ISBN 80-7202-6046.**
3. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. 1. vyd. Zlín : Univerzita Tomáše Bati, Fakulta technologická, 2003. 64 s.**
4. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. 2. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 123 s.**
5. **ŘÍHA, Milan, SIEGER, Ladislav. Bezpečnostní systémy. 3. vyd. Praha : Námořní akademie České republiky, 2009. ISBN 978-80-87103-21-0.**
6. **HULVA, Tomáš. Ochrana majetku. Praha : Linde, 2008. 375 s. ISBN 978-80-7201-712-6.**
7. **KAMENÍK Jiří, BRABEC František a kolektiv. Komerční bezpečnost : soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. 1. vyd. Praha : ASPI, 2007. 338 s. ISBN 978-80-7357-309-6.**
8. **KONÍČEK, Tomáš. Zabezpečení automobilů. Praha : Policie ČR, 2005. 32 s.**
9. **KORANDA, Vladimír. Porušování povinností při správě majetku soukromoprávních subjektů. 1. vyd. Praha : Eurolex Bohemia, 2005. 165 s. ISBN 80-86861-34-1.**

Vedoucí diplomové práce: **Ing. Radek Šilhavý, Ph.D.**
Ústav počítačových a komunikačních systémů

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

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Ve své diplomové práci se budu zabývat problémem počítačové kriminality vztažené na finanční sektor, ve kterém mám více zákazníků a i já sám jsem v něm zaměstnán. V teoretické části rozeberu pojmy a postupy potřebné pro vytvoření skenovacího systému. V praktické části pak zjištěné problémy a analýzy reportů, včetně prezentace jejich řešení.

Klíčová slova:

počítačová kriminalita, skenovací systém, IT, finanční sektor

ABSTRACT

In my work I deal with the problem of cyber crime related to the financial sector, where I have more customers and even I am employed in it. In the theoretical part I look at the concepts and procedures needed for a scanning system. The practical part is about founded problems and analysis of reports, including presentations of their solutions.

Keywords:

computer crime, the scanning system, IT, financial sector

Poděkování

Na tomto místě bych chtěl poděkovat své přítelkyni a rodině za podporu, kterou mi věnovali. Dále chci poděkovat svému vedoucímu diplomové práce za konzultace a podnětné návrhy.

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

Zabezpečení počítačů a ochrana dat je nekončící proces, neboť v průběhu času se mohou ve výchozím nastavení bezpečnostního systému nebo v jeho obsluze objevit slabiny, které mohou způsobit, že tento systém selže a data uniknou nebo systém umožní jejich modifikaci neoprávněným uživatelem.

Informační technologie jsou v dnešní době asi nejpoužívanějším artiklem moderního člověka. Mnoho lidí si již svět bez IT nemůže představit. Stále více a více svěřujeme svým pevným diskům citlivá data ať již ze svého soukromého, nebo pracovního života. S tím ovšem souvisí problém počítačové kriminality, který se prohlubuje spolu s vývojem informačních technologií.

V této diplomové práci se zaměřuji na problém krádeží a záměny hardwarových komponent. V teoretické části se zabývám pojmem počítačová kriminalita a způsoby jakými monitorovat změny v hardware konfiguraci stanic. Dále nastiňuji problém, který se vyskytl u jednoho mého zákazníka a byl odhalen pomocí řešení popsaném v této práci. Při samotné implementaci a po jejím nasazení se ukázalo, že řešení není komplexní, a proto se v praktické části této práce zabývám řešením nalezených problémů z výstupu ze systému.

Součástí této diplomové práce je také CD se zdrojovými kódy v systému popisovaném v této práci.

I. TEORETICKÁ ČÁST

1 POČÍTAČOVÁ KRIMINALITA

Pokud se bavíme o počítačové kriminalitě musíme rozlišit dva pohledy na tento problém. Jedním je počítačová kriminalita ve smyslu užití počítače jako nástroje pro provedení kriminálního činu. V rámci této oblasti se můžeme nejčastěji setkat s pojmy jako je [2]:

- Neoprávněné užití cizí věci [1] – trestný čin neoprávněného užívání cizí věci je definován naším právním systémem podle §207 trestního zákoníku (zákon číslo 40/2009 sbírky). O neoprávněném přístupu k počítačovému systému a nosiči informací pak hovoří §230 trestního zákoníku (zákon číslo 40/2009 sbírky).
- Hacking – pronikání do systémů
- Carding – zneužití čipové karty
- Hoax – šíření poplašné zprávy
- Spamming – zasílání nevyžádané pošty
- Warez – autorská díla, se kterými je nakládáno nelegálně, zejména v rozporu s autorským zákonem

Těmi se mi v této práci zabývat nebudeme (nebo je případně pouze okrajově zmíníme jako možnou hrozbu).

Druhý pohled na počítačovou kriminalitu je získání počítače, nebo jeho části neoprávněným způsobem, neboli jeho zcizení, poškození. Do této kategorie můžeme zařadit pojmy [3]:

- Krádež [1] – podle §205 trestního zákoníku (zákon číslo 40/2009 sbírky) je v souvislosti s počítači možné mluvit o trestném činu krádeže především tehdy, dojde-li k odcizení celého počítače. Výpočetní technika má obecně značnou hodnotu, a tudíž je pro zloděje velmi atraktivním artiklem. Nemusí dojít pouze ke krádeži počítače, terčem mohou být například díly ještě nesestaveného počítače, záznamová média (pokud jsou prázdná), příslušenství apod.

- Loupež [1] – o loupeži můžeme hovořit ve smyslu §173 trestního zákoníku (zákon číslo 40/2009 sbírky) například tehdy, pokud bude při přepadení lupičem odcizen notebook, či jiný podobný předmět.

- Poškození cizí věci [1] – poškození cizí věci mluvíme v souvislosti s §228 trestního zákoníku (zákon číslo 40/2009 sbírky), pouze pokud se nebude jednat o záznam na nosiči informací.

- Poškození záznamu v počítačovém systému a na nosiči informací a zásahu do vybavení počítače z nedbalosti – o tomto problému hovoří §232 trestního zákoníku (zákon číslo 40/2009 sbírky). Jedná se například o zničení, poškození, pozměnění, nebo učinění neupotřebitelnými dat uložených přímo v počítačovém systému nebo na nosiči informací. [3]

Páchání zločinů má několik důvodů, jako je například získání citlivých informací, poukázání na chyby v systému, a jiné. Nejčastějším stále zůstává získání finančních prostředků pro další kriminální aktivity. Proto se pozornost zločinců stále častěji ubírá směrem k sektorům, které obsahují velké peníze – finanční sektor [4].

1.1 Bezpečnost [5]

Pod tímto pojmem si můžeme představit situaci anebo stav, ve kterém chráněnému objektu nehrozí žádné nebezpečí, či nevnikají žádné škody ať už přímo na objektu, nebo jeho obsahu. Teoreticky můžeme říci, že tento objekt je pod totálním zabezpečením.

Totální zabezpečení neexistuje v reálném světě, neboť v něm jsme vystaveni neustálým hrozbám. Pokud tedy mluvíme o zabezpečení objektu, mluvíme o reálné bezpečnosti, při které jsou minimalizována rizika ztráty, poškození, zničení, či jiná míra hrozícího nebezpečí.

1.2 Bezpečnost v IT [6]

Ohledně bezpečnosti v IT existuje několik směrnic, které jsou návody, jak zabezpečit například firmu, či její informační systém. O tyto směrnice se starají organizaci z nichž nejznámější je Český normalizační institut (http://www.cni.cz).

1.2.1 ČSN ISO/IEC 27000

Bezpečnostní normy jsou důležitým prvkem informační bezpečnosti. Cílem této řady norem označených ISO/IEC 27000 je sjednotit požadavky, návody a doporučení na systémy řízení informační bezpečnosti, které se vyskytují v různých normách.

Základní, sjednocující normou je ISO/IEC 27001:2005. Norma poskytuje doporučení a specifikuje požadavky, jak aplikovat vybraná opatření ISO/IEC 17799:2005 (do budoucna ISO/IEC 27002) v rámci procesu ustavení, provozu, údržby a zlepšování systému managementu bezpečnosti informací v organizaci. Norma poskytuje model pro zavedení efektivního systému řízení bezpečnosti informací (ISMS - Information security management system) v organizaci a doplňuje tak normu ISO 17799. Norma dále prosazuje procesní přístup k řešení ISMS a zavádí model známý pod zkratkou PDCA (Plan-Do-Check-Act).

1.2.2 ČSN ISO/IEC TR 13335-1 (Pojetí a modely bezpečnosti IT)

Část 1 poskytuje přehled základních pojetí a modelů, použitých k popisu řízení bezpečnosti IT. Tento materiál je vhodný pro manažery odpovědné za bezpečnost IT a pro ty, kdo jsou odpovědní za celkový bezpečnostní program organizace.

1.2.3 ČSN ISO/IEC TR 13335-2 (Řízení a plánování bezpečnosti IT)

Část 2 popisuje řídící a plánovací aspekty. Tato část má význam pro manažery s odpovědnostmi souvisejícími se systémy IT organizace. Těmi mohou být manažeři IT, kteří jsou odpovědní za dohled nad návrhem, implementací, testováním, pořízením nebo provozováním systémů IT nebo manažeři, kteří jsou odpovědní za činnosti, které využívají podstatným způsobem systémy IT.

1.2.4 ČSN ISO/IEC TR 13335-3 (Techniky pro řízení bezpečnosti IT)

Část 3 popisuje bezpečnostní techniky vhodné pro použití pracovníky, kteří jsou zapojeni do manažerských činností v průběhu životního cyklu projektu, jako je plánování, návrh, implementace, testování, získání nebo provozování.

1.2.5 ČSN ISO/IEC TR 13335-4 (Výběr ochranných opatření)

Část 4 poskytuje směrnice pro výběr ochranných opatření s ohledem na potřeby činnosti organizace a problémy bezpečnosti a jak může být tento výběr podporován použitím základních modelů a kontrol. Popisuje proces výběru ochranných opatření podle bezpečnostních rizik, problémů a specifického prostředí organizace. Ukazuje, jak dosáhnout odpovídající ochrany a jak může být tento proces podporován aplikací základní úrovně bezpečnosti. Poskytuje i vysvětlení, jak přístup naznačený v této části podporuje techniky pro řízení bezpečnosti IT předložené v ISO/IEC TR 13335-3.

1.3 Audit [7]

Před zahájením jakýchkoliv změn v infrastruktuře, či pravidelné údržby je třeba provézt úvodní audit stavu výpočetní techniky. Audit nám pomůže zmapovat aktuální stav IT a odhalit bezpečnostní rizika. [5]

V oblasti IT by měl obsahovat tyto části:

- Hardwarový audit – tento audit byl jedním z důvodů vypracování této diplomové práce
- Softwarový audit
- Bezpečnostní audit

Výsledkem auditu by pak mělo být odhalení bezpečnostních rizik, zavedení neustále aktuální evidence nejen počítačů, ale i nainstalovaného software, počtu zakoupených licencí, jednotlivých instalací a majetku. Přenesení zodpovědnosti za nainstalovaný software na uživatele, pokud tato skutečnost již neexistuje, abychom si tak optimalizovali množství finančních prostředků investovaných do kontrol. Přehled využí-

vaných licencí nám pak může poukázat na nutné nákupy licencí (legalizace), či jejich budoucí neprodlužování. Odhalení nainstalovaného nelegálního software, nebo software zakázaného vnitřní politikou firmy. [7]

1.3.1 Hardwarový audit [7]

V první fázi musíme shromáždit všechny dostupné informace o hardware, který je použitý v dané organizaci. Pro účely této diplomové práce použijeme následující typy zařízení:

- Server
- Desktopová stanice
- Notebook / laptop

Sběr těchto dat provedeme pomocí specializovaného nástroje a jako výsledek z tohoto software budeme mít přehledný seznam všech zařízení včetně podrobného přehledu nainstalovaného hardware a software.

V druhé fázi je vhodné tyto informace odborně posoudit a porovnat se strategickými cíly společnosti. Je možné, že by pro zamýšlený účel vyhovovala jiná struktura zařízení. Aktuální seznam zařízení je zároveň nutným podkladem pro stanovení metody a frekvence údržby zařízení.

1.3.2 Softwarový audit [7]

Softwarový audit čerpá z podkladů zjištěných v průběhu hardwarového auditu. Zjednodušeně při něm dochází k evidenci používaného software, odhalení nelegálně využívaného software a posouzení vhodnosti aktuální licenční politiky vzhledem k cílům společnosti. K tomuto auditu můžeme opět užít specializovaného nástroje. Jako jeden z vedlejších efektů softwarového auditu můžeme dostat převod odpovědnosti za legálnost nainstalovaného software na zaměstnance podniku, pokud již tato skutečnost není aplikována. Zatím ve všech firmách a zákazníků, u kterých jsem pracoval, byla tato

skutečnost již zavedena a zaměstnanec ji při nástupu podepisoval seznámení s vnitřní směrnicí, či samostatný dokument, ve kterém mu byla tato skutečnost prezentována.

1.3.3 Bezpečnostní audit [7]

Cílem bezpečnostního auditu by mělo být především odhalení bezpečnostních rizik provozování vaší výpočetní techniky. V Bezpečnostním auditu bychom se dle mého názoru měli zaměřit zejména na následující oblasti:

- Pravidelná aktualizace operačních systémů
- Pravidelná aktualizace antivirových a antispywarových systémů
- Spolehlivé zálohovací mechanismy
- Ochrana dat a firemní bezpečnostní politika
- Ochrana proti průniku z internetu
- Fyzické zabezpečení infrastruktury

Odstranění zjištěných bezpečnostních rizik by mělo předcházet veškeré další činnosti.

2 FINANČNÍ SEKTOR [10]

Do finančního sektoru v České republice můžeme zahrnou veškeré instituce, které se řídí zákonem o bankách (zákon 21 /1992 sbírky) – Českou národní banku, komerční banky, dále pak Ministerstvo financí, pojišťovny, penzijní fondy, družstevní záložny, investiční společnosti, investiční fondy, …

V tomto sektoru se nenachází prostředky pouze několika jedinců, ale většiny občanů České republiky. Kdo z nás nemá účet v bance, či uzavřené spoření u některého peněžního ústavu. Případně si nezaložil životní pojistku, nebo neinvestoval do cenných papírů / fondů.

Největší rozmach počítačové kriminality v tomto odvětví zaznamenala média v USA v letech 2006 – 2008 [4]. Bohužel ani dnes není zabezpečení natolik dokonalé, a proto k této kriminální činnosti stále dochází. Například v únoru tohoto roku došlo k vynesení informací o účtech Švýcarské banky Credit Suisse, jejím vlastním zaměstnancem. Německá vláda dokonce oficiálně nabídla 2.3 milionů liber za ukradený disk, aby tak získala informace o účtech a měla tak přístup k ukrytým penězům z neplacených daní (předpoklad je 400 milionů liber). [8]

V České republice se bankovní sektor zaměřuje spíše na internetovou kriminalitu a zamezení získání informací neoprávněnou osobou pomocí komunikačních nástrojů, případně pomocí programu, který žádané informace pomůže útočníkovi získat. Varianta krádeže informací na jiném nosiči, případně krádež zařízení obsahujícího citlivá data, není mnohdy kontrolována vůbec, což je problém. [9]

3 BOJ S POČÍTAČOVOU KRIMINALITOU

Boj s počítačovou kriminalitou se nikterak neliší od boje s jakoukoliv jinou formou kriminality. Pro naše potřeby v této práci ji můžeme rozdělit na dvě části, a to prevence a represe. Podle mého názoru nemůže jedna bez druhé existovat a nalézt optimální podíl zastoupení těchto částí při minimalizaci počítačové kriminality je obtížné. Jsem přesvědčen, že pokud je kladen vyšší důraz na prevenci, pak není třeba zavádět tolik represivních opatření a tím dochází k nejen finančním úsporám. Navíc díky problémům s objasňováním zločinů spojených s počítačovou kriminalitou (například krádež nehmotného majetku) je působení represe velmi omezené.

„Je třeba přesunout daleko více sil do oblasti prevence, ochrany počítačů a informačních systémů, neboť jedině tak lze účinně bojovat proti tomuto druhu trestné činnosti … .“ [11]

Při boji s počítačovou kriminalitou si musíme primárně ujasnit, jak budeme postupovat, co chceme chránit a jakým způsobem. Přitom využíváme vlastních zkušeností a řídíme se příslušnými normami a legislativou.

3.1 Prevence [1]

Existuje několik pohledů na prevenci a její dělení. Pro účely této práce nám postačí velmi jednoduché dělení na *psychologickou prevenci* a na *technologickou prevenci*.

3.1.1 Psychologická prevence

Pokud se bavíme o psychologické prevenci, máme na mysli takové kroky (soubor pravidel), či opatření, které zvyšují povědomí o trestných činech a následcích za jeho prokázání. Literatura hovoří o takzvaném *zvyšování stupně společenské akceptace práva*, neboli podpoře jedné ze stránek právního vědomí subjektů práva:

„Druhou stránkou právního vědomí jsou názory na to, co je spravedlivé a co ne-spravedlivé, resp. co a jak by mělo či nemělo být regulováno pomocí práva, jaké zájmy, či hodnoty by mělo právo zajišťovat, či potlačovat apod. (de lege ferenda)“ [12]

3.1.2 Technologická prevence

Technologickou prevenci můžeme chápat jako jakoukoliv uměle přidanou ochranu, neboli zabezpečení, ať už na fyzické, či nefyzické úrovni. Příkladem mohou být různé zámky, či čidla, ale také několik variant skenování hardware pomocí software.

Metody skenování a jejich problémy, se kterými jsem se setkal, si probereme v praktické části této diplomové práce.

Jakákoliv uměle přidaná ochrana, která není zakomponována do návrhu fyzického zařízení, komponenty, či programu nedostatečná – místy až bezcenná. [1]

3.2 Represe

Pro zajištění této oblasti boje s počítačovou kriminalitou existují v našem státě státní orgány činné v trestních řízeních. Jedná se především o Policii České republiky a soudní systém. Úkolem těchto orgánů je vyšetřování přestupků a trestných činů, jejich objasňování a ukládání sankcí dle zákonu v příslušném zákoníku.

Represe může fungovat pouze za předpokladu, že vyřešení deliktu bude rychlé a správné, stejně jako určení trestu, které bude navíc ještě úměrné závažnosti provinění. Obecně však můžeme říci, že pachatelé trestných činů jsou stále o kousek před jejich objasňovateli a tedy mnohdy se represe míjí účinkem, neboť nedojde ke včasnému potrestání, nebo dokonce k objasnění zločinu. [5]

4 METODY ZJIŠŤOVÁNÍ HARDWARE

K tomu, abychom mohli zjistit, zda došlo či dochází ke krádežím, je nutné evidovat stav zařízení v jistých časových intervalech a tyto stavy průběžně kontrolovat a porovnávat.

4.1 Technologie WIM [13]

WMI - Windows Management Instrumentation je infrastruktura pro správu dat a operací na operačních systémech založených na Windows. WMI využívá CIM (Common Information Model) repositář pro standardní reprezentaci systémů, aplikací, síťových zařízení, hardware a ostatních spravovatelných komponent. CIM je vytvořeno (při instalaci počítače) a spravováno pomocí DMTF (Distributed Management Task Force).

K informacím z WMI lze přistupovat pomocí WMI objektů a metod. Standardní uživatel má přístup k WMI pouze ke čtení informací, Administrátor pak i k zápisu.

Pomocí služby vzdálená správa systému Windows – WinRM (Windows remote management) – se lze k modelu WMI připojit i z jiného počítače. Tuto možnost lze využít například při hromadné kontrole některých údajů (např. kdo je aktuálně přihlášený k počítači, jak dlouho počítač běží, atd,.)

4.2 Registr operačního systému Windows [14]

Jedná se o centrální hierarchickou databázi, která se používá v operačních systémech Microsoft Windows 98, Windows CE, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7 a v ekvivalentních rodinách serverů založených na technologii NT a slouží k ukládání informací potřebných ke konfiguraci systému pro jednoho či více uživatelů, aplikací a hardwarových zařízení.

Registr obsahuje informace, které systém Windows neustále používá během operací, jako jsou například profily jednotlivých uživatelů, aplikace nainstalované v počítači a typy dokumentů, které mohou jednotlivé aplikace vytvářet, nastavení stránek vlastností

složky a ikony aplikací, informace o hardwaru existujícím v systému a o používaných portech.

Registr nahrazuje většinu textových souborů INI používaných v systému Windows 3.x a konfiguračních souborů systému MS-DOS, jako jsou například soubory Autoexec.bat a Config.sys. I když naleznete registr v několika operačních systémech Windows, existují mezi nimi určité rozdíly.

Mezi základní kořenové klíče registrů patří [14]:

- *HKEY_CLASSES_ROOT* - Tento klíč obsahuje informace týkající se asociace názvů souborů, informací OLE (Object Linking and Embedding) a asociací tříd souborů.

  OLE se používá k výměně dat mezi jednotlivými aplikacemi.

- *HKEY_CURRENT_USER* - Obsahuje aktivní profil uživatele, který je právě přihlášen do systému (nastavení plochy, sítě apod.) Odpovídá tedy části z HKEY_USERS.

- *HKEY_LOCAL_MACHINE* - Obsahuje hardwarové profily. Je to kořenový klíč, který obsahuje nastavení pro všechny uživatele a nastavení systému.

- *HKEY_USERS* - Zahrnuje všechny aktivní profily, včetně HKEY_CURRENT_USER.

- *HKEY_CURRENT_CONFIG* - Součástí tohoto klíče jsou informace o konfiguračních datech aktuálního hardwarového profilu.

- *HKEY_PERFORMANCE_DATA* - Tento klíč není zobrazen v editoru registru a jsou v něm uložena data kernelu (jádro systému) samotných Windows.

- *HKEY_DYN_DATA* - Tento klíč je použit pouze u operačních systémů Windows 95, Windows 98 a Windows Me. Obsahuje informace o hardwaru, včetně Plug and Play zařízení.

Podregistr registru je skupina klíčů, podklíčů a hodnot v registru, která má sadu pomocných souborů obsahujících záložní kopie jejích dat. Pomocné soubory pro všechny podregistry kromě HKEY_CURRENT_USER jsou uloženy ve složce %SystemRoot%\Sys-

tem32\Config v systémech Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 a Windows Vista. Pomocné soubory pro podregistr HKEY_CURRENT_USER jsou uloženy ve složce %SystemRoot%\Profiles\Uživatelské_jméno. Přípony názvů souborů v těchto složkách označují typ obsažených dat. Také chybějící přípona může někdy označovat typ obsažených dat.

Podregistr registru	Pomocné soubory
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Tabulka 1: Registry systému Windows a jejich uložení na disku

V systému Windows 98 se soubory registru nazývají User.dat a System.dat. V systému Windows Millennium Edition se soubory registru nazývají Classes.dat, User.dat a System.dat.

4.3 SNMP [16]

SNMP je jednoduchý, široce rozšířený a užitečný standardizovaný protokol, který slouží k získávání nebo nastavování hodnot na určitém zařízení. Obdobou je například WMI od firmy Microsoft. Podporu SNMP má velká řada zařízení, například aktivní síťové prvky, počítačová čidla, tiskárny, přístupové body nebo pomocí softwaru a ovladačů ji mohou získat osobní počítače a servery. Hodnoty můžeme získávat v pravidelném intervalu a ty pak jednoduše ukládat do databáze spolu s časem a následně vykreslit do grafu. Přehledně tak můžeme zobrazit třeba vytížení procesoru, průběh teploty nebo datový tok na portu přepínače.

Protokol SNMP vyžaduje pro komunikaci dvě strany. Jednou entitou je správce (manager) a druhou agent. SNMP pracuje ve dvou režimech činnosti [15]:

- Správce posílá dotazy agentovi a přijímá odpovědi. Hodnoty tedy může získávat i více správců a mohou se ptát kdykoliv.
- Agent zasílá oznámení (trapy) na adresu správce. V nějakých definovaných situacích (překročení nějaké hodnoty nebo i v pravidelném intervalu) odesílá agent jednomu správci hodnoty.

Protokol SNMP nyní existuje ve třech verzích. SNMPv1 a SNMPv2c používají pro autentizaci community string, v podstatě textové heslo. V SNMPv3 je možno využít autentizaci pomocí jména a hesla a šifrování.

SNMP používá pro komunikaci UDP protokol, díky čemuž je velmi rychlé, ale může dojít ke ztrátě (nedoručení) zasílané informace (paketu). Od verze 2 je implementována kontrola doručení, takže ke ztrátě by nemělo dojít. Standardně se používá port 161 (SNMP) na straně agenta (pro dotazy) a port 162 (SNMPTRAP) na straně serveru (pro trapy). Klient, který posílá dotaz, zvolí dynamický port, z kterého posílá dotaz na port 161. Agent odpovídá z portu 161 na dynamický port klienta. V praxi je pro každý dotaz použit jiný dynamický port.

4.4 Příkazy operačního systému Linux [17]

V operačním systému Linux přímo existují zabudované příkazy, které nám ulehčí výpis aktuálního hardware. Aktualizace tohoto výpisu je prováděna při zavádění operačního systému do paměti a nebo během daemona kudzu.

Některé distribuce Linuxu podporují výpis pomocí přehledné tabulky, kterou lze zobrazit pomocí příkazu *$ lshw.*

Příkaz	Význam
$ cat /proc/cpuinfo	zobrazení informací o CPU
$ free -m	zobrazení informací o paměti
# lspci	zobrazení všech PCI zařízení
# lsusb	zobrazení všech USB zařízení
$ lsdev	více informacích o zařízeních

Tabulka 2: Některé příkazy OS Linux pro zobrazení nainstalovaného HW

5 PROJEKT ZABEZPEČENÍ MINIMALIZACE ZTRÁT V OBLASTI IT V POJIŠŤOVNĚ A BANCE

Ve své praxi jsem dostal za úkol vytvořit pro účely vnitřního auditu, u několika nejmenovaný bank a pojišťoven, základní řešení pro zjištění, zda došlo ke zcizení části některého počítače / laptopu, nebo se jednalo o úmyslnou změnu, která byla například provedena pracovníkem IT. K tomuto určení mi bylo řečeno, že budou užity speciální osoby, která budou kontrolovat reporty z mé aplikace. Jak se později ukázalo z těchto reportů, jeden ze subjektů z finančního sektoru mohl přijít o část svých peněz vlivem počítačové kriminality. Tento projekt se pak u tohoto zákazníka stal součástí hardwarového auditu. [18]

5.1 Zadání projektu pro vnitřní audit [18]

„V rámci vnitřního auditu je třeba řešit otázku sledování zda nedochází ke zcizení sledovaného hardware z vybraných pracovních stanic / laptopů (lehce konfigurovatelné). Vyhodnocení bude zpracování formou reportu, který vybraný zaměstnanec jednou za určené období vyhodnotí. Sledovaný hardware: základní deska (BIOS), CPU, paměti, pevné disky a CD / DVD mechanika. Skupina počítačů, která se bude skenovat je dynamické a její změna musí být jednoduchá a bude ve správě týmu, který se stará o Active Directory (AD). Monitorovací systém bude nasazen a použit pro monitorování pracovních stanic na kterých jsou instalovány pouze operační systémy od společnosti Microsoft, a to ve verzích Windows 2000 až Windows Vista.“ Až při pozdější komunikaci zákazník určil, že pro skenování sledovaných stanic lze užít pouze prostředků VB skriptu.

5.2 Problémy navrženého systému

Již při dokončení projektu bylo zřejmé, že nepokrývá veškeré problémy, které zákazník má a že toto řešení bude nutné do budoucna doladit a rozšířit, aby sloužilo svému účelu v plné míře. Dle mého názoru by také mohl externí audit tento systém označit za nedůvěryhodný a doporučit provedení změn do dalšího auditu.

5.2.1 Neúplnost dat

Pokud se podíváme na data, která získáme ze skenovacího skriptu, zjistíme, že některá zařízení nemají vyplněna sériová čísla. Ani předělání skenování z komunikace s WMI na procházení registrů nám v tomto ohledu nepomůže, neboť informace nejsou v zařízení zavedena již od výrobce. Díky tomuto problému pak nejsme například schopni rozlišit od sebe dvě stejné paměti nebo dva pevné disky.

5.2.2 Redundance

Pro sériová čísla máme i tento problém. Jelikož výrobce vyprodukuje mnoho kusů výrobku dochází v některých případech k takzvané redundanci sériových čísel, kdy dva různé kusy stejného výrobku mají stejné sériové číslo. Jednak tímto ztrácíme jednoznačný identifikátor zařízení a dále pak nejsme schopni v několika případech zjistit, že došlo k záměně.

5.2.3 Odpojitelná zařízení = nepřehlednost reportu

Jelikož u zákazníka je povoleno používat flash disky a různá jiná odpojitelná zařízení do USB dochází v reportu ke generování odebírání a přidávání zařízení (disku). Tyto akce pak znepřehledňují celý report a systém se tak stává nepoužitelným pro zjištění, zda došlo k odcizení hardware.

5.2.4 Proměnná rychlost procesoru

Jednou z klíčových informací o procesoru je jeho rychlost. U notebooku dochází k její změně například při odpojení napájecího kabelu. To znamená, že v reportu dojde k identifikaci záměny procesoru za jiný. Také u některých pevných stanic existuje technologie (například AMD Cool and quiet), která reguluje takt procesoru dle jeho vytížení.

5.2.5 Vypnutá zařízení – krádež celého zařízení?

Pokud se podíváme na situaci, kdy dojde k delšímu odstavení koncového zařízení (manager odjíždí na služební cestu i se svým laptopem, nemocný člověk nepřijde do práce

a počítač je vypnutý), systém toto vyhodnocuje jako krádež celého zařízený a vyvolá falešný poplach – do reportu je zaznamenáno celé zařízení jako odebrané.

5.2.6 Non-Windows operační systémy

Jelikož je skenovací skript založen na technologiích Microsoft Windows, není tento použitelný pro jiné operační systémy. Tedy nelze tímto skriptem skenovat například Linux, či Unix, který je používán převážně v serverových řešeních. Dále v sítích najdeme síťové tiskárny, které používají většinou jako svůj operační systém různé mutace *NIXových distribucí.

II. PRAKTICKÁ ČÁST

6 AUDIT ZÁKAZNÍKŮ

Pro evidenci majetku používají zákazníci program Správce IT od společnosti MiCOS Software (www.micos-sw.cz). Zakoupené licence k tomuto programu jsou ale použity k evidenci majetku pouze v režimu offline (zakoupeno je pouze deset základních licencí). Tedy nedochází k žádnému skenování vzdálených stanic online a opakovaně pak dle nastaveného časového harmonogramu, ale pouze k prvotnímu naskenování provedeného ručním spuštěním skenování na dané stanici a jeho následném importu do programu Správce IT. Jelikož oba zákazníci, jak pojišťovna tak banka používají pro správu jednu organizaci, která zavedla standardizaci do správy IT a navrhla kompletní zabezpečení obou organizací, můžeme k těmto subjektům přistupovat obdobným způsobem.

6.1 Tabulky o výsledcích hardwarového auditu

V následujících tabulkách se podíváme na výsledky naskenovaného majetku pomocí následujícího postupu:

1. Technik IT pomocí GPO politik zaslal na všechny počítače evidované na doménovém řadiči spuštění skenovacího klienta.
2. Po naskenování hardware došlo k nahrání skenů do sdílený prostor na distribuovaný souborový systém.
3. Technik IT provedl import skenů do programu Správce IT, čímž aktualizoval databázi evidovaného majetku.
4. Společně s technikem jsme rozdělili majetek do několik skupin.

Majetek	Počet aktivních kusů
Servery	175
Počítačová stanice – kritická	3000
Počítačová stanice – standardní	12000
Periferní zařízení (tiskárny připojené, nebo síťové)	5000
Celkem	**20175**

Tabulka 3: Hardwarový audit majetku u zákazníka banka

Majetek	Počet aktivních kusů
Servery	25
Počítačová stanice – kritická	1800
Počítačová stanice – standardní	3200
Periferní zařízení (tiskárny připojené, nebo síťové)	500
Celkem	**5525**

Tabulka 4: Hardwarový audit majetku u zákazníka pojišťovna

U jednotlivých skupin jsou samozřejmě stanoveny periody kontrol. Pokud se podíváme na nejkratší interval z těchto kontrol, zjistíme, že se jedná o jeden měsíc a to pomocí instalace aktualizací na jednotlivé stanice a servery.

7 POPIS PROJEKTU NA SKENOVÁNÍ HARDWARE

7.1 Skenovací a reportovací systém

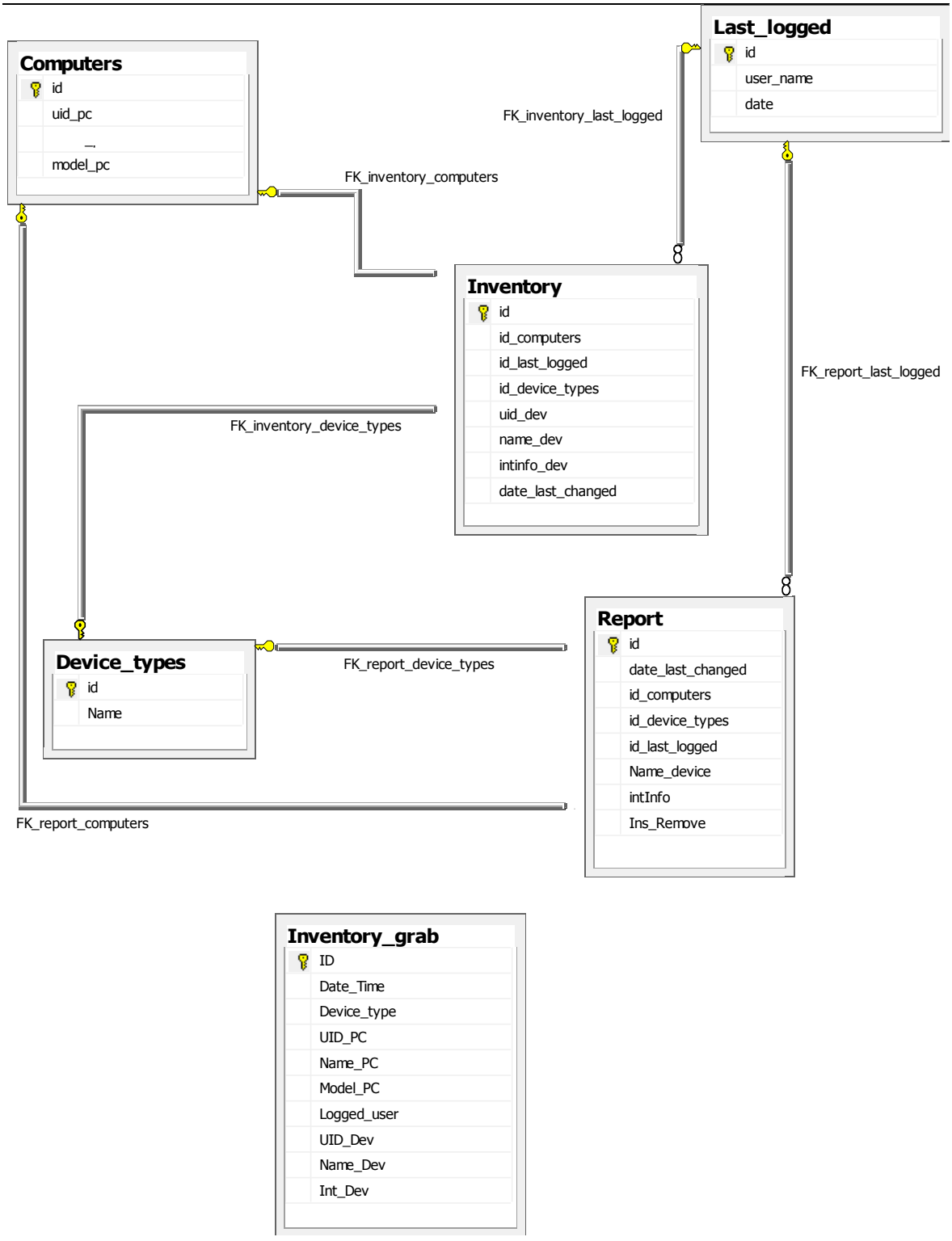
Na základě zadání byl vytvořen projekt, který obsahuje několik částí – skenovací skript, databáze pro ukládání skenů, reportovací aplikaci a zobrazení reportu.

7.1.1 Skenovací skript

Jelikož organizace potřebovala rychlé a levné řešení, bylo použito pro vytvoření skriptu pro skenování nainstalovaného hardware na stanici jednoduchého jazyka „visual basic script“. Skenování probíhá na základě komunikace skriptu s WMI rozhraním. Skript je zašifrovaný základní šifrou od společnosti Microsoft (vbe) – Microsoft Script Encoder (screnc.exe) – tedy pro lidské oko není viditelný zdrojový kód. Propagace skriptu je pomocí Group policy (GPO) pouze na určenou skupinu počítačů (je použita počítačová politika GPO).

7.1.2 Datové úložiště

Jako datové úložiště po komunikaci se zákazníkem byla zvolena databáze Microsoft SQL ve verzi 2005, která byla již u zákazníka licencována. Na této úrovni bylo důležité zabývat se přístupy k datům, aby nedocházelo k nechtěnému zveřejnění informací, či případným změnám ve výsledcích skenování. K tomuto účelu byl vypracován systém uživatelských jmen a nastavení jejich oprávnění pro přístup do databáze.



Obrázek 1: Návrh databáze - schéma

Přihlašování k databázi je tvořeno dvoufázově. Jelikož skenovací skript běží pod stejnými právy jako je přihlášený uživatel / účet počítače mají tyto skupiny účtů povoleno připojení k databázovému serveru. Pro práci s databázovými objekty je pak užit interní

uživatel SQL HwWriter (viz „Nastavení práv na datové úložiště“), pro kterého jsou nastavena oprávnění.

Popis jednotlivých tabulek a významu sloupců:

Inventory_grab – vstupní tabulka pro skenovací skript.

- ID – jedinečný identifikátor
- Date_time – datum a čas, kdy byl proveden sken
- Device_type – typ naskenovaného zařízení (BIOS, paměť, disk, …)
- UID_PC – jedinečný identifikátor počítače – složený z Name_PC a Model_PC
- Name_PC – hostname počítače
- Model_PC – model počítače (HP Compaq dc7700, Optiplex 755, …)
- Logged_User – uživatel přihlášený v době skenování počítače
- UID_Dev – jedinečný identifikátor zařízení – složený z Name_Dev a IntDev (pokud existuje)
- Name_Dev – název naskenovaného zařízení
- IntDev – číselná hodnota popisující zařízení

Computers – tabulka obsahující informace o počítačích – aktuální stav.

- ID – jedinečný identifikátor
- UID_PC – jedinečný identifikátor počítače – složený z Name_PC a Model_PC
- Name_PC – hostname počítače
- Model_PC – model počítače (HP Compaq dc7700, Optiplex 755, …)

Last_logged – tabulka obsahující informace o přihlášených uživatelích

- ID – jedinečný identifikátor
- User_name – uživatelské jméno složené ze jména domény a uživatelského jména

- Date – datum posledního přihlášení uživatele – poslední odeslaný sken s daným uživatelem

Device_types – tabulka typů zařízení, které byly naskenovány.

- ID – jedinečný identifikátor
- Name – název typu zařízení

Inventory – tabulka spojení a jednotlivých zařízení, která informuje jaký byl poslední zapamatovaný stav daného zařízení, jeho komponent a poslední přihlášený uživatel na tomto zařízení v době skenování

- ID – jedinečný identifikátor
- Id_computers – odkaz na tabulku počítačů
- Id_last_logged – odkaz na tabulku posledních přihlášených uživatelů
- Id_device_types – odkaz na tabulku typů zařízení
- UID_Dev – jedinečný identifikátor zařízení – složený z Name_Dev a IntDev (pokud existuje)
- Name_Dev – název naskenovaného zařízení
- IntDev – číselná hodnota popisující zařízení
- Date_last_changed – datum kdy bylo zařízení naposledy reportováno – naskenováno

Report – tabulka obsahující reporty vytvořené reportovacím programem na základě porovnávání změn mezi jednotlivými skeny

- ID – jedinečný identifikátor
- Date_last_changed – datum kdy byla zjištěna skutečnost evidovaná v reportu
- Id_computers – odkaz na tabulku počítačů
- Id_last_logged – odkaz na tabulku posledních přihlášených uživatelů

- Id_device_types – odkaz na tabulku typů zařízení
- Name_device – Název zařízení u kterého došlo ke změně
- IntInfo – číselná hodnota popisující zařízení
- Ins_remove – typ zjištěné akce (-1 – došlo k odebrání, 1 – došlo k přidání)

7.1.3 Nastavení práv na datové úložiště

Abychom mohli v projektu minimalizovat riziko zneužití dat, existují na databázi tři uživatelé:

- HwWriter je uživatel, který má právo pouze zápisu naskenovaných informací do tabulky Inventory_grab a je využívám pouze skenovacím skriptem
- HwReporter, který má právo pouze pro čtení z tabulek report, device_types, computers a last_logged a je použit pro zobrazování reportů
- HwManager, který má právo zápisu a čtení ve všech tabulkách. Tento uživatel je využíván aplikací pro porovnávání

7.1.4 Aplikace pro porovnávání

Tato aplikaci je naprogramována v jazyce C# pro .NET verze 2. Obsahuje veškerou logiku pro vytváření reportu z naskenovaných dat porovnávaných s posledním známým stavem.

Spuštění této konzolové aplikace je prováděno pomocí nástroje „naplánované úlohy“, který je součástí Microsoft Windows Serveru 2003 ze kterého je spuštění aplikace prováděno. Aplikace běží v kontextu servisního účtu, který je vyplněn na kartě naplánované úlohy.

Na základě komunikace se zákazníkem byl plán nastaven na jednodenní spouštění ve 20:00.

7.1.5 Aplikace pro porovnávání – struktura po instalaci aplikace

- *Sync.EDA.HwInfo.Reporter.exe* – spustitelný soubor aplikace
- *Sync.EDA.HwInfo.Reporter.exe.xml* – konfigurační soubor aplikace. Obsahuje nastavení potřebné pro běh aplikace, jako je připojení k databázi, nastavení logování, seznam podporovaného hardware, … .
- *Sync.EDA.HwInfo.Global.dll* – podpůrná knihovna pro udržení nastavení aplikace.
- *Sync.EDA.HwInfo.Helper.dll* – podpůrná knihovna obsahující metody pro práci s logovacím souborem.
- *Sync.EDA.HwInfo.dbConnector.dll* – podpůrná knihovna ve které nalezneme jádro pro porovnávání.
- *Sync.EDA.HwInfo.dbConnector.MSSQL.dll* – podpůrná knihovna pro práci s databází MSSQL.
- *Log* – adresář ve do kterého je ukládán logovací soubor, v případě, že je zapnuto logování aplikace. Můžeme tu najít také staré logovací soubory.

7.1.6 Aplikace pro porovnávání – popis konfiguračního souboru

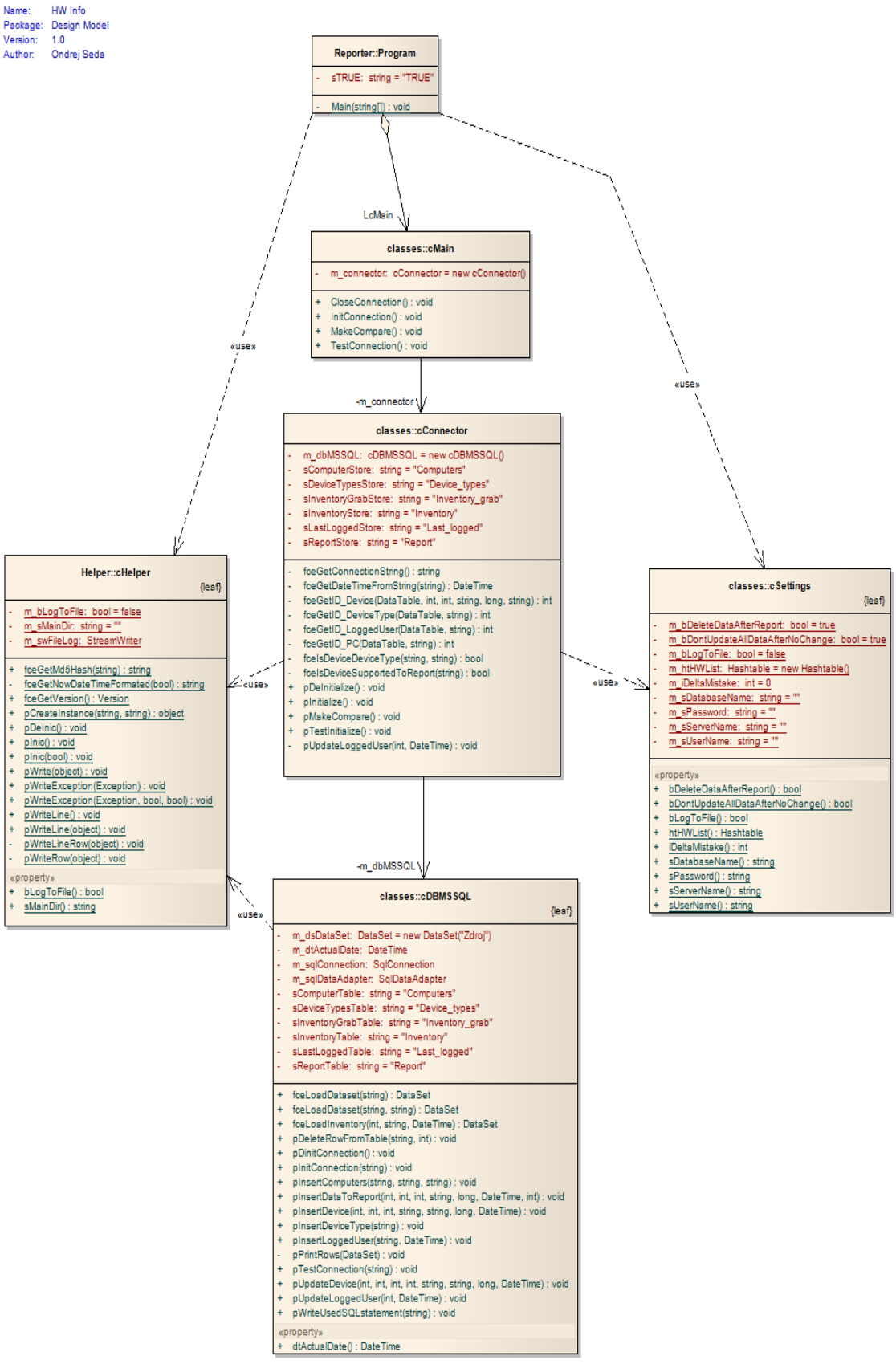
```
<?xml version="1.0"?>
<configuration>
    <configSections>
        <section name="HWList" type="System.Configuration.NameValueSectionHandler"/>
    </configSections>
    <startup>
        <supportedRuntime version="v2.0.50727" />
    </startup>
    <HWList>
        <add key="CPU" value="CPU" />
```

```
            <add key="HDD" value="Hard Drive" />
            <add key="MEM" value="Physical Memory" />
            <add key="DVD" value="CD/DVD drive" />
            <add key="BIOS" value="BIOS" />
        </HWList>
        <appSettings>
            <add key="bLogToFile" value="true" />
            <add key="bDeleteDataAfterReport" value="true" />
            <add key="bDontUpdateAllDataAfterNoChange" value="true" />
            <add key="sServerName" value="localhost" />
            <add key="sDatabaseName" value="hwinventory" />
            <add key="sUserName" value="HWAudit_operator" />
            <add key="sPassword" value="cFjnf K1215sdJh" />
            <add key="iDeltamistake" value="10" />
        </appSettings>
</configuration>
```

- *?xml* – informuje o použitém standartu XML jazyka
- *Configuration* – sekce obsahující vškeré nastavení pro aplikaci a prostředí do kterého bude aplikace spouštěna.
- *ConfigSections* – informuje o uživatelsky vytvořených sekcích, v konfiguračním souboru, které lze číst za běhu programu a o jejich typech.
- *Startup* – seznam kontrol, které se provedou při startu. V této ukázce se kontroluje zda existuje verze .NET frameworku verze 2.0 alespoň build 50727. Framework pak sam rozpozná, zda podporuje tuto verzi (například pokud je na stanici verze 3 SP 1) a podle toho vyvolá hlášení a nebo povolí spuštění.
- *HWList* – uživatelská sekce čtená aplikací. V této je nutné definovat seznam podporovaného hardware aplikací – tj. Hardware, který se bude kontrolovat a

reportovat. Jednotlivé typy hadrware jsou evidovány ve tvaru klíč (jedinečný záznam) a název. Název se musí schodovat s názvem zapisovaným do tabulky Inventory_grab.

- *AppSettings* – v této sekci je nastavení, jak se má aplikace zachovat.
  - *bLogToFile* – povolení logování do souboru v podadresáři "Log".
  - *bDeleteDataAfterReport* – povolení smazání zdrojových dat po jejich zpracování
  - *bDontUpdateAllDataAfterNoChange* – nastavení frekvence aktualizace informací v paměti při práci aplikace.
  - *sServerName* – jméno počítače na kterém běží databáze MSSQL.
  - *sDatabaseName* – název schématu, ke kterému se aplikace připojí. V tomto schématu musí existovat struktura tabulek včetně nastavení přístupových práv.
  - sUserName – uživatelské jméno sloužící pro připojení se ke schématu.
  - sPassword – heslo pro připojení k databázi zapsáno jako čitelný text. Ochrana tohoto hesla je pomocí standartních prostředků operačního systému Windows, a to nastavením práv na daný soubor.
  - iDeltaMistake – některé procesory nepodporující snižování své frekvence vykazují při více nasjenováních odchylku o 1MHz. Tento parametr slouží pro ignorování tohoto rozdílu. Příklad: Pokud potřebujeme nastavit rozdíl 10MHz, znamená to, že hodnota iDeltaMistake musí být rovna 5. Tj. +5 a -5.



Obrázek 2: Diagram tříd aplikace pro porovnávání

7.1.7 Aplikace pro porovnávání – popis struktury aplikace

Program – třída, která je vstupem do programu. Po spuštění ihned dojde ke zpracování vstupní metody „Main“.

- Main() – v této metodě načteme konfigurační soubor a provedeme inicializaci logování do adresáře *Log*, pokud je tato volba zapnuta. Řízení pak předáme do instance třídy cMain.

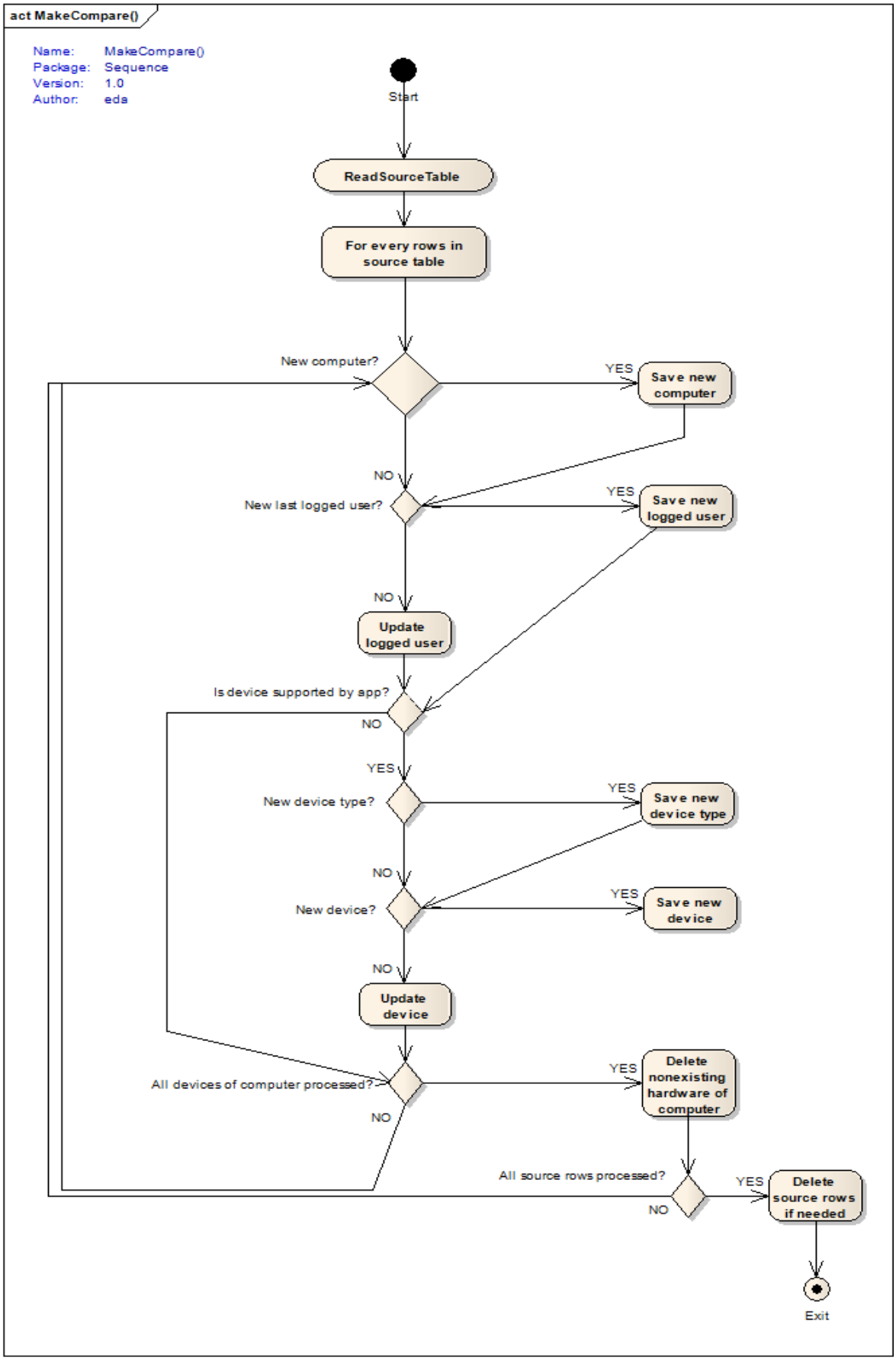
cMain – třídou oddělujeme exe soubor od dalším podpůrných DLL knihoven. Veškeré požadavky přesměrováváme na třídu *cConnector*.

- InitConnection() - v této metodě inicializujeme připojení k databázi.
- TestConnection() - tuto metodu použijeme pro otestování připojení se k databázi, vypsání informací o databázi a instanci a nakonec odpojení.
- MakeCompare() - tímto spustíme proces porovnávání a vytváření reportu k připojené databázi.
- CloseConnection() - pro odpojení se od databáze a uzavření logovacího souboru použijeme tuto metodu.

cConnector – v této třídě máme jádro celé aplikace, a to konkrétně v metodě MakeCompare().

- fceGetConnectionString() - metoda provede sestavení připojovacího řetězce k databázi.
- fceGetDateTimeFromString() - převede řetěz na datový typ datetime.
- fceGetID_Device() - vrátí ID pro zařízení.
- fceGetID_DeviceType() - vrátí ID pro typ zařízení.
- fceGetID_LoggedUser() - vrátí ID pro uživatele.
- fceGetID_PC() - vrátí ID pro počítač.
- fceIsDeviceDevice() - vrátí zda je zařízení daného typu

- fceIsDeviceSupportedToReport() - metoda vrátí, zda je typ zařízení podporovaný pro zpracování do reportu.
- pInitialize() - v této metodě inicializujeme připojení k databázi pomocí databázového objektu.
- pTestInitialize() - tuto metodu použijeme pro otestování připojení se k databázi, vypsání informací o databázi a instanci a nakonec odpojení.
- pMakeCompare() - tímto spustíme proces porovnávání a vytváření reportu k připojené databázi. Na vstupu si program načte záznamy z tabulky Inventory_grab, které byly uloženy do doby jeho spuštění. Nové informace postupně plní do struktury tabulek propojených s tabulkou Inventory. Pokud se jedná o úplně nový počítač, není do reportu zahrnut, v opačném případě jsou do tabulky reportů vkládány informace, zda došlo k přidání, či odebrání hardware. Podle nastavení jsou data ve zdrojové tabulce buď smazána, nebo ponechána.
- pDeinitialize() - pro odpojení se od databáze a uzavření logovacího souboru použijeme tuto metodu.



Obrázek 3: Popis práce metody pMakeCompare()

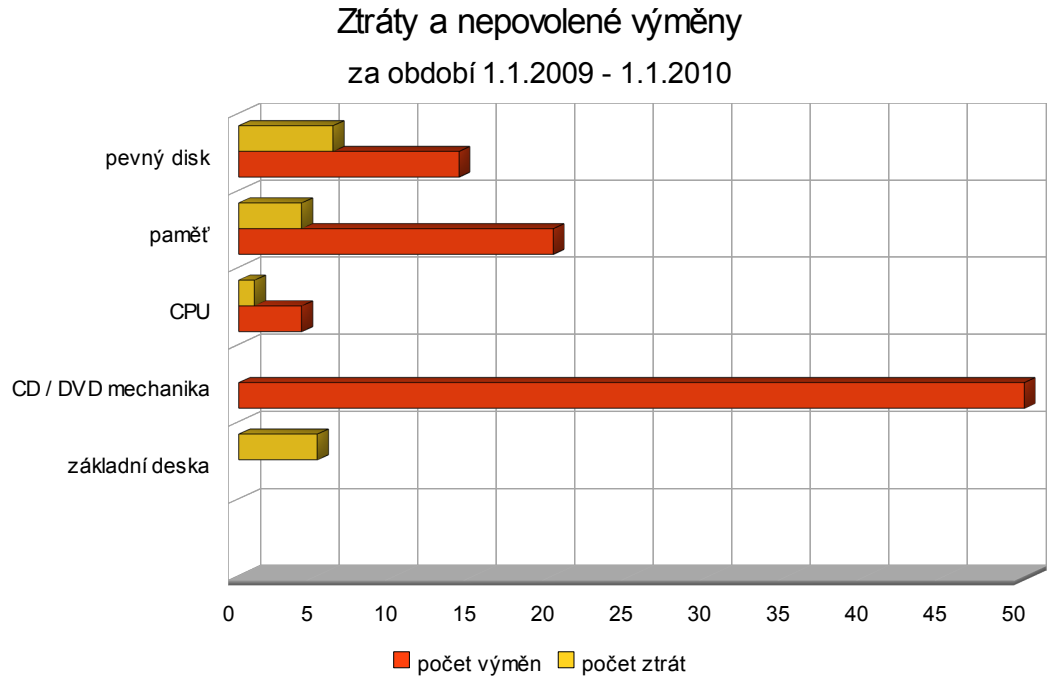
cDBMSSQL – v této třídě máme definovány jednotlivé postupy jakým způsobem uloží aplikace data do databáze, provede jejich modifikaci, či načtení a nebo mazání. Pro účely této diplomové práce není třeba abychom si popisovali význam jednotlivých metod v této třídě.

cHelper – tato pomocná statická třída využívána ze všech částí programu. Obsahuje metody pro práci s logovacím souborem, zobrazování chybových hlášení, pomocné metody pro práci s datem nebo s verzí programu.

cSettings – tato statická třída drží nastavení programu načtené z konfiguračního souboru po celou dobu běhu aplikace. Tyto informace pak využíváme z větší části programu.

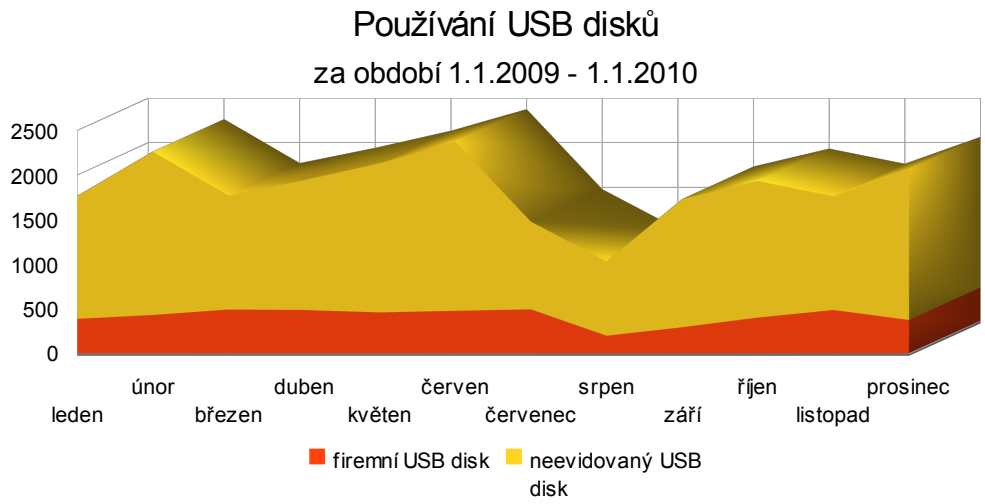
7.2 Výsledky projektu – analýza rizik

Výsledek projektu – report společně s kontrolou evidence hardware – mimo problémů ukázal také neschválené změny v konfiguraci některých strojích pracovníků informačních technologií a dokonce i jiných stojích o které měli starost pečovat. Několik zaměstnanců si dokonce z této činnosti udělalo výnosný obchod (pobočkové stanice). Tento problém se projevil pouze u zákazníka banky.



Obrázek 4: Ztráty a nepovolené výměny hardware u stanic zákazníka

Další problém, který projekt odhalil bylo nadměrné a nekontrolovatelné používání externích disků / flashdisků i u uživatelů, kteří ke své práci tyto zařízení nepotřebují a od zákazníka je nemají ani přidělena u obou zákazníků (jak banka, tak pojišťovna).



Obrázek 5: Používání USB disků za rok 2009 u zákazníků.

Zákazníci registrují ve své evidenci přibližně 600 kusů USB zařízení a to včetně vyřazených. Ve svých školeních a vnitřních předpisech dokonce zakazují užívání vlastních zařízení – tedy se zjevně jedná o porušení vnitřních předpisů a to ve velkém množství.

7.3 Výsledky projektu – postoj zákazníka

V pracovním řádu má zákazník zakotveny podmínky a informace o tom, jak naložit s lidmi, kteří poškodí firmu z pohledu finančních operací. Ohledně krádeží a jiné nelegální činnosti se pak odkazují na trestní a občanský zákoník. Jakýkoliv takovýto čin bezprostředně předává policii a ukončuje pracovní poměr se zaměstnancem.

8 NAVRŽENÉ ZMĚNY

U zákazníků existuje tedy několik problémů, které je třeba řešit.

1. Ztráty, či neřízené záměny hardware
2. Problémy skenovacího systému
3. Porušování vnitřního předpisu o zákazu užívání vlastních zařízení

8.1 Porušení vnitřního předpisu o užívání USB disků

Pokud se podíváme na tento problém, zjistíme, že omezením používání USB disků vyřešíme několik bezpečnostních aspektů:

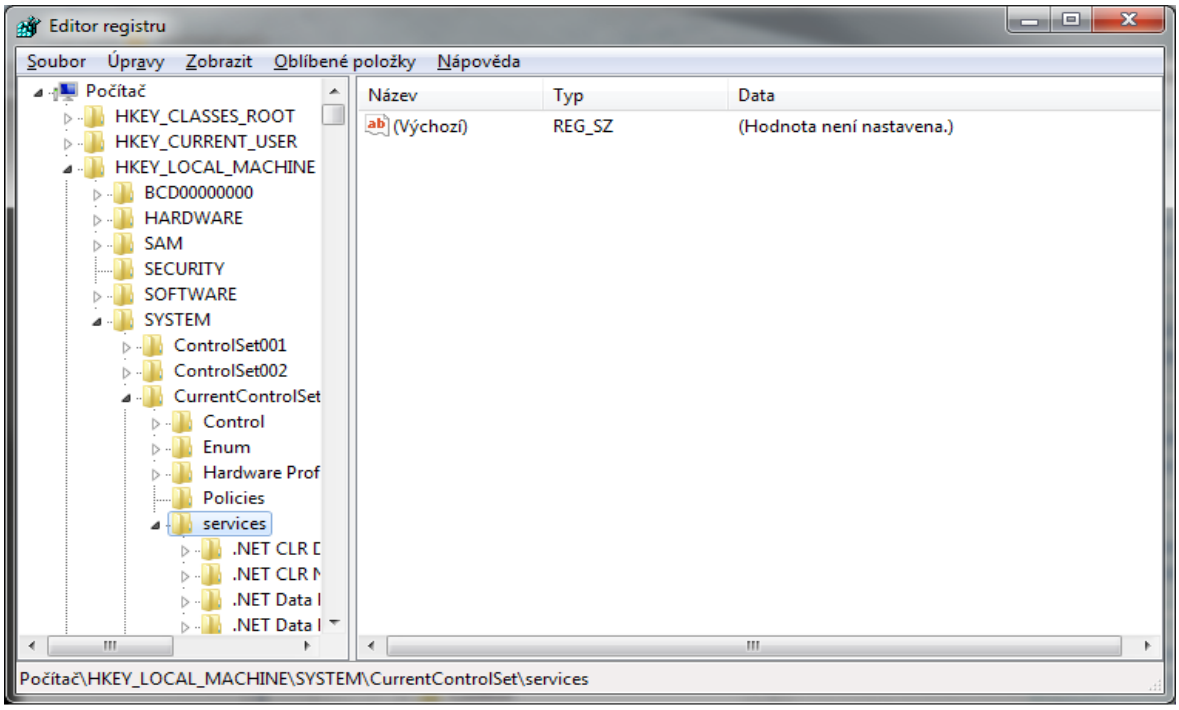
- Vynášení interních materiálů zákazníka (email je již plně monitorován, co se týče obsahu)
- Šíření nelegálního obsahu po interní síti (na výstupních a vstupních bodech pracují proxy servery, které filtrují nelegální obsah)

Pro řešení tohoto problému můžeme použít v oblasti Windows nastavení politiky GPO na uživatelské skupiny (tj. na uživatele, nikoliv na počítač), nebo zakázat spouštění služby USBSTOR, která se stará o správu USB zařízení a jejich práci.

Pokud chceme **zakázat kompletně** používání USB úložišť na jednotlivých počítačích (lokální nastavení), použijeme k tomuto účelu registry systému Windows [19].

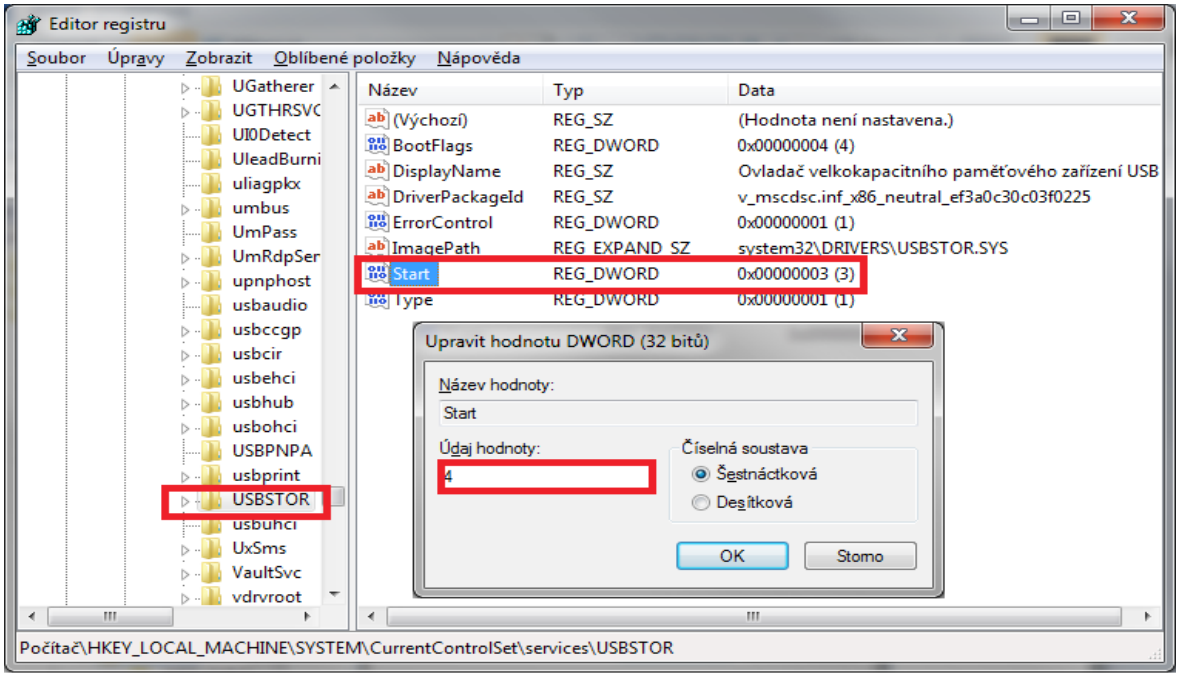
- Spustíme nástroj *regedit.exe* pro úpravu lokálních registrů v administrátorském režimu
- Veškeré služby a ovladače, které jsou zaváděny při startu systému Windows se nachází v cestě zobrazené na obrázku níže (obr. 6).
- V této větvi musíme nalézt klíč USBSTORE (Ovladač velkokapacitního paměťového zařízení USB) a v něm položku *Start*
- Změnou hodnoty této položky ze 3 (povoleno manuální spouštění) na 4 (zakázáno) docílíme, že po znovuspouštění systému nebudou načteny

k dispozici ovladače USB a tímto nebudeme moci na dané stanici používat žádné zařízení používající tohoto rozhraní.



Obrázek 6: Cesta ke službám a ovladačům operačního systému MS Windows

- Změnu nastavení položky start vidíme na obr. 7.



Obrázek 7: Zakázání načítání ovladače pro práci s USB

Toto nastavení nasadíme u zákazníka pro stanice, které nejsou připojeny přímo do interní sítě (tj. spravovány doménovým kontrolerem), ale jsou na nich využívány jeho aplikace pracující s informacemi zákazníka (takzvané terminály). Tyto informace mají sloužit pouze pro prohlížení a nikoliv k další distribuci.

Pro zakázání používaní USB zařízení zaměstnancům pracujících v interní síti, využijeme politiky GPO (všechny klientské stanice pracují na operačním systémy MS Windows 2000 nebo MS Windows XP, v nové síti pak MS Windows Vista).

Pro DC (doménový kontroler) postaveném na Windows 2008 již existuje podpora přímo v GPO. Jelikož zákazník využívá služeb i serverů postavených na starších operačních systémech Windows, je tato doména kontrolována a spravována DC z MS Windows 2003, ve kterém bohužel neexistuje přímo podpora pro zakázání USB. Tuto podporu zapneme importem ADM souboru, který je v příloze 1 součástí této diplomové práce. Postup máme tedy následující [19]:

- Otevřeme na DC konzolu *Group policy management console*.
- Vytvoříme novou politiku a zeditujeme ji.
- Do sekce *Administrative templates* přidáme ADM soubor z přílohy 1 nebo z přílohy 2 (pro mého zákazníka použijeme obě tyto předlohy, neboť některé stanice budou mít zakázány i jiná zařízení kromě USB) této diplomové práce
- Uložení GPO
- Nastavení použití GPO objektu na skupinu

8.2 Problémy skenovacího systému – non-Windows OS

Aktuální použití skenovacího systému nedovoluje spravovat jiné než Windows operační systémy. Zákazník ovšem používá pro produkční databáze *NIXové operační systémy a do budoucna plánuje jejich kontrolu. Proto doporučuji rozšířit systém o SNMP kontrolu těchto systémů (veškeré servery běží v datových centrech v interní síti zákazníka). Agent v *NIXových systémech je standardně podporován, a proto budeme potřebovat pouze naprogramování SNMP čtečky, která bude ukládat data do databáze.

Jako alternativu můžeme navrhnout vytvoření klienta přímo pro danou verzi *NIXového systému za pomocí příkazů z tab. 1 a tab. 2. Tuto variantu můžeme použít například v odloučených pracovištích.

8.3 Problémy skenovacího systému – nepřehlednost reportu

Jako řešení tohoto problému navrhuji rozšířit reportovací aplikaci o funkcionalitu takzvaného blacklistu – tj. zařízení (jejich jméno) nebude zpracován reportovací aplikací, i když vyhovuje vstupním podmínkám pro skenovaný hardware. Bude nutné rozšířit konfigurační soubor o sekci HWexclude:

```
<HWexclude>
        <add key="CPU" value="" />
        <add key="HDD" value="%flash%;%SmartWare%;%Jogr%" />
        <add key="MEM" value="" />
        <add key="DVD" value="" />
        <add key="BIOS" value="" />
</HWexclude>
```

kde znak procenta (%) bude určovat libovolný počet znaků ednotlivé položky pak budeme oddělovat znakem středníku (;). Seznam podporovaných sekcí bude vypadat následovně:

```
<configSections>
        <section name="HWList" type="System.Configuration.NameValueSectionHandler"/>
        <section name="HWexclude" type="System.Configuration.NameValueSectionHandler"/>
</configSections>
```

Kontrolu budeme provádět ve třídě *cConnector* v metodě *pMakeCompare()*, kterou rozšíříme o patřičný kód. Jednotlivými sekcemi v HWexclude pak určíme na jaký typ zařízení se filtr bude aplikovat. Načítání sekce HWexclude provedeme stejně jako u sekce HWList v metodě *Main* třídy *Program*.

8.4 Ostatní problémy

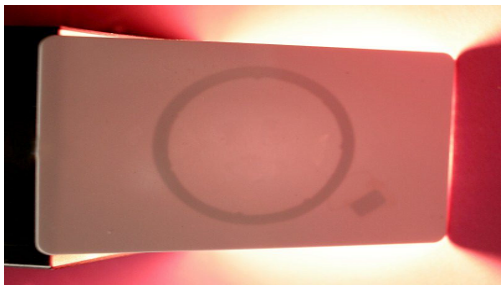
Jak můžeme vidět pouze softwarové řešení nedokáže komplexně ochránit zákazníka. Z tohoto důvodu musíme přistoupit rozšíření systému o samotné fyzické zabezpečení jednotlivých stanic. [20]

8.4.1 Identifikace osob

Pokud rozšíříme kontrolu vstupu a výstupu osob z perimetru i do vnitřních prostor (zóny okolo serveroven, vstup do sekce IT, …), dostaneme tak lepši přehled o pohybu osob po objektu. K tomuto účelu lze užít například bezkontaktních identifikačních karet vycházejících z čipových karet. [20]

Čipová karta [21] – jedná se o integrovaný zalisovaný obvod do nosiče (např. plastikový obal) obsahující kryptografický koprocesor s dostatečně velkou pamětí (RAM, ROM, EEPROM) a software (operační systém čipu). V čipu dochází ke generování privátního klíče, který slouží pro komunikaci, ale nikdy neopustí obvody karty.

Bezkontaktní karta [22] – vizuálně bezkontaktní plastové karty vypadají jako obyčejné karty, ale uvnitř plastu mají zalisovanou elektronickou soustavu složenou z čipového modulu a kruhové nebo obdélníkové antény. Bezkontaktní plastové karty mají většinu výhod čipových karet, ale převyšují je vysokou odolností na vlhkost a mechanické opotřebení, neboť komunikace s čtečkou je bezkontaktní. Životnost karet je několik let. Lze je bezproblémově provozovat i v prašném prostředí. Napájení má indukční charakter a je zprostředkováno z čtečky. V návaznosti na typ čipového modulu a použité čtečky můžou karty komunikovat jednostranně (jenom čtení) nebo oboustranně (čtení/zápis).



Obrázek 8: Bezkontaktní karta

8.4.2 Štítky a radiofrekvenční systémy [23]

Tato dvoupólová ochrana se skládá ze dvouanténního systému, který se připevní na hlídané zařízení a z kontrolní brány, kterou umístíme u vchodů a východů. Při průchodu branou je signalizován poplach (tichý a nebo akustický). Nasazen tohoto systému se nám vyplatí do míst s velkým průchodem lidí. Pro datová centra se nám bude hodit skenovací komora.

8.4.3 Skenovací komora – do datového centra [24]

Obrázek 9: Skenovací komora

Kontrolní systém těchto komor je založen na porovnávání subjektu při vstupu a výstupu z objektu. Subjekt se do komory hlásí pomocí své identifikační karty. Po vstupu je naskenován, zvážen a jeho profil uložen k předchozím. Poté je subjekt vpuštěn do objektu. Při východu z budovy dochází opět k naskenování a porovnání s předchozími skeny. Pokud je rozpoznán rozdíl je informována ostraha a subjekt se musí vrátit a podrobit se další kontrole. [25]

8.4.4 Zámek na počítač [24]

Obrázek 10: Zámek na počítač

Poskytuje fyzické a vizuální zastrašení proti krádeži – pozinkovaným ocelovým lanem připojíme notebook k zabezpečenému objektu. Lze použít pro většinu notebooků, ploché obrazovky, projektory, DVD vypalovačky a jinou cennou elektroniku.

ZÁVĚR

Problém počítačové kriminality si v dnešní době jistě zaslouží svou pozornost a měl by být diskutován jak mezi lajckou veřejností, tak orgány činnými v trestním řízení. Od diskuzí by pak mělo dojít k zvýšení zabezpečení ať již hardwarového, nebo softwarového vlastnictví.

V úvodní části jsem zpracoval pohled na počítačovou kriminalitu jako celek a její dělení se specializací se na bezpečnost a bezpečnost v IT. Dále se obracím k finančnímu sektoru ve kterém jsem osobně také zaměstnán. V teoretické části se pak ještě zabývám bojem s počítačovou kriminalitou a metodami zjišťování hardware na stanici. V poslední části této kapitoly popisuji motivaci k vytvoření systému na skenování hardware a reportování změn.

V praktické části jsem se snažil vyřešit problémy, které se vyskytly po nasazení systémů a také nalezené v reportech. Problémy jsem rozdělil do třech skupin (úprava aplikace, úprava prostředí a fyzické zabezpečení) což mi pomohlo úspěšně nalézt jejich řešení.

Výsledky této práce budou navrženy pro implementaci do prostředí zákazníka a věřím, že alespoň některé z nich budou akceptovány.

RESUME IN ENGLISH

The problem of cyber crime have today certainly deserve our attention and should be discussed between both – public authorities and law enforcement. The discussions should then lead to increase of security, whether hardware or software ownership.

In the first section, I compiled an insight into cyber-crime as a whole and its divisions, specializing in the safety and security in IT. Next I have turned my view to the financial sector in which I am personally also employed. The theoretical part is more involved in combating cyber crime detection methods and hardware to the station. In the last section of this chapter I described the motivation for the system of scanning hardware and reporting changes.

In the practical part, I tried to solve the problems that occurred after the deployment of system and also problems found in the reports. The problems I have divided into three groups (treatment applications, modification of the environment and physical security), which helped me to successfully find their solutions.

The results of this work will be proposed for implementation in the customer environments and I believe that at least some of them will be accepted.

bc. Ondřej Šeda

SEZNAM POUŽITÉ LITERATURY

[1] MATĚJKA, Michal. *Počítačová kriminalita*. První vydání. Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2.

[2] RYBIČKA, Doc. Jiří *Počítačová kriminalita - počítačové viry*. In *Počítačová kriminalita. Informatika pro ekonomy II. přednáška 7* [online]. Brno : PEF MZLU, 2008 [cit. 2010-06-06]. Dostupné z WWW: <https://akela.mendelu.cz/~rybicka/prez/viry.ppt>.

[3] *Businesscenter.cz* [online]. 2009 [cit. 2010-06-06]. Trestní zákoník. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/trestni-zakonik/>.

[4] *Privacy rightsclearinghouse* [online]. 20.4.2005, 4.6.2010 [cit. 2010-06-06]. Chronology of Data Breaches. Dostupné z WWW: <Chronology of Data Breaches>.

[5] LAUCKÝ, JuDr. Vladimír. *Technologie komerční bezpečnosti I*. Zlín : UTB - Academia Centrum Zlín, 2004. 64 s. ISBN 80-7318-194-0.

[6] *Standardy* [online]. 2007 [cit. 2010-06-06]. Bezpečnost IS/IT. Dostupné z WWW: <http://www.itil.cz/index.php?id=1003>.

[7] *Audit PC* [online]. 2009 [cit. 2010-06-06]. Softwarový audit, Hardwarový audit. Dostupné z WWW: <http://www.audit-pc.cz/>.

[8] *Interní školení a školící materiály zákazníka*

[9] *Businesscenter.cz* [online]. 1991 [cit. 2010-06-06]. Zákon o bankách. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/banky/>.

[10] *Businesscenter.cz* [online]. 1991 [cit. 2010-06-06]. Zákon o bankách. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/banky/>.

[11] SMEJKAL, Vladimír *Informační a počítačová kriminalita v České republice* [online]. 1999 [cit. 2010-01-01]. Dostupné z WWW: <http://www.mvcr.cz/casopisy/studie/diskuze/analyza.html>.

[12] BOGUSZAK, Jiří; ČAPEK, Jiří. *Teorie práva*. Praha : Codex Bohemia, 1997. 150 s.

[13] MSDN [online]. 5.4.2010 [cit. 2010-06-06]. O WMI. Dostupné z WWW: <http://msdn.microsoft.com/en-us/library/aa384642(v=VS.85).aspx>.

[14] *Technická podpora Microsoft* [online]. 2006, 12.3.2008 [cit. 2010-06-06]. Informace o registru systému Windows pro pokročilé uživatele. Dostupné z WWW: <http://support.microsoft.com/kb/256986/cs>.

[15] *Www.samuraj-cz.com : fórum* [online]. 20.12.2006 [cit. 2010-06-06]. SNMP - Simple Network Management Protocol. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/>.

[16] *DPS Telecom* [online]. 2006 [cit. 2010-06-06]. SNMP Tutorial: An Introduction to SNMP. Dostupné z WWW: <http://www.dpstele.com/layers/l2/snmp_tutorials.php>.

[17] NEMETH, Evi; SNYDER, Garth; HEIN, Trent R. *Linux : Kompletní příručka administrátora*. První vydání. Brno : Computer press, 2004. 828 s.

[18] *Interní materiály zákazníka*

[19] RUSSEL, Charlie; CRAWFORD, Sharon. *Microsoft Windows Server 2008 : Velký průvodce administrátora*. První vydání. Brno : Computer press, 2009. 1272 s.

[20] *Security World.cz : Deník o bezpečnosti pro IT profesionály. Zabezpečení firemních sítí, serverů, internetová bezpečnost* [online]. 2009 [cit. 2010-06-06]. Http://www.securityworld.cz. Dostupné z WWW: <http://www.securityworld.cz>.

[21] *T-SOFT* [online]. 2009 [cit. 2010-06-06]. Bezpečnostní technologie. Dostupné z WWW: <http://www.tsoft.cz/cipove-karty>.

[22] *Daficard : dodavatel a výrobce plastikových karet* [online]. 14.10.2009 [cit. 2010-06-06]. Druhy plastových karet. Dostupné z WWW: <http://www.daficard.cz/druhy-plast-karet/>.

[23] *American Security : Advanced EAS Systems & Accessories* [online]. 2008 [cit. 2010-06-06]. Elektronické systémy RF. Dostupné z WWW: <www.americansecurity.cz>.

[24] *ArchiExpo* [online]. 2010 [cit. 2010-06-06]. Products. Dostupné z WWW: <http://www.archiexpo.com/>.

[25] *Par-Kut international* [online]. 2010 [cit. 2010-06-06]. Booths. Dostupné z WWW: <http://www.parkut.com/>.

[26] *Technical support Microsoft* [online]. 8.6.2005 [cit. 2010-06-06]. HOWTO: Use Group Policy to disable USB, CD-ROM, Floppy Disk and LS-120 drivers. Dostupné z WWW: <http://support.microsoft.com/kb/555324>.

Další zdroje nepoužité přímo:

- JÜTTNER, Alfred. O kriminologii a kriminalitě. 1. vyd. Praha : Orbis, 1968. 214 s. Zákony II/2009 : sborník úplných znění zákonů obchodního, občanského a trestního práva a souvisejících předpisů platných k 1.1.2009. Český Těšín : Poradce, 2009. 848 s.
- DIEM, Walter. Bezpečnostní zařízení. Praha : Ikar, 2000. 110 s. ISBN 80-7202-6046.
- LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. 2. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 123 s.
- ŘÍHA, Milan, SIEGER, Ladislav. Bezpečnostní systémy. 3. vyd. Praha : Námořní akademie České republiky, 2009. ISBN 978-80-87103-21-0.
- HULVA, Tomáš. Ochrana majetku. Praha : Linde, 2008. 375 s. ISBN 978-80-7201-712-6.
- KAMENÍK Jiří, BRABEC František a kolektiv. Komerční bezpečnost : soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. 1. vyd. Praha : ASPI, 2007. 338 s. ISBN 978-80-7357-309-6.
- KONÍČEK, Tomáš. Zabezpečení automobilů. Praha : Policie ČR, 2005. 32 s.
- KORANDA, Vladimír. Porušování povinností při správě majetku soukromoprávních subjektů. 1. vyd. Praha : Eurolex Bohemia, 2005. 165 s. ISBN 80-86861-34-1.
- KOKOREVA, Olga. Registr Microsoft Windows XP : Kompletní průvodce přizpůsobením a optimalizací operačního systému. Computer Press, 2002. 414 s. ISBN 80-7226-783-3.

bc. Ondřej Šeda

- HORÁK, Jaroslav. Hardware učebnice pro pokročilé : 3. aktualizované vydání. Computer Press, 2005. 348 s. ISBN 80-251-0647-0.
- ALTIRIS® Notification Server 6.0 SP3 : Help., [2005]. 201 s. Dostupný z WWW: http://www.altiris.com/upload/notificationsp3.pdf.
- http://www.cni.cz
- http://www.bsi-global.com
- http://www.iso.org

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OS	Operační systém
HW	Hardware
SW	Software
IT	Informační technologie
WMI	Windows Management Instrumentation
CIM	Common Information Model
DMTF	Distributed Management Force Task
WinRM	Windows Remote Management
SNMP	Simple Network Management Protocol
$	Linux shell commander
#	Linus bash commander
CPU	Central Processing Unit
AD	Active Directory
DC	Domain controller
GPO	Group Policy Object model
VBE	Visual Basic Encrypted
VBS	Visual Basic Script
SQL	Standard Query Language
MS	Microsoft
USB	Universal Serial Bus
*NIX	Unix, Linux, … - distribuce postavené na jádře Unixu a nebo Linuxu

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ADM SOUBOR PRO ZPŘÍSTUPNĚNÍ ZAKÁZÁNÍ VŠECH DISKŮ – STANDARTNĚ VŠE POVOLENO [26]

```
CLASS MACHINE

CATEGORY !!category

 CATEGORY !!categoryname

  POLICY !!policynameusb

   KEYNAME "SYSTEM\CurrentControlSet\Services\USBSTOR"

   EXPLAIN !!explaintextusb

     PART !!labeltextusb DROPDOWNLIST REQUIRED


       VALUENAME "Start"

       ITEMLIST

        NAME !!Disabled VALUE NUMERIC 3 DEFAULT

        NAME !!Enabled VALUE NUMERIC 4

       END ITEMLIST

     END PART

   END POLICY

  POLICY !!policynamecd

   KEYNAME "SYSTEM\CurrentControlSet\Services\Cdrom"

   EXPLAIN !!explaintextcd

     PART !!labeltextcd DROPDOWNLIST REQUIRED


       VALUENAME "Start"

       ITEMLIST

        NAME !!Disabled VALUE NUMERIC 1 DEFAULT

        NAME !!Enabled VALUE NUMERIC 4

       END ITEMLIST
```

```
    END PART
  END POLICY
 POLICY !!policynameflpy
  KEYNAME "SYSTEM\CurrentControlSet\Services\Flpydisk"
  EXPLAIN !!explaintextflpy
    PART !!labeltextflpy DROPDOWNLIST REQUIRED

      VALUENAME "Start"
      ITEMLIST
       NAME !!Disabled VALUE NUMERIC 3 DEFAULT
       NAME !!Enabled VALUE NUMERIC 4
      END ITEMLIST
    END PART
  END POLICY
 POLICY !!policynamels120
  KEYNAME "SYSTEM\CurrentControlSet\Services\Sfloppy"
  EXPLAIN !!explaintextls120
    PART !!labeltextls120 DROPDOWNLIST REQUIRED

      VALUENAME "Start"
      ITEMLIST
       NAME !!Disabled VALUE NUMERIC 3 DEFAULT
       NAME !!Enabled VALUE NUMERIC 4
      END ITEMLIST
    END PART
  END POLICY
END CATEGORY
```

```
END CATEGORY


[strings]
category="Custom Policy Settings"
categoryname="Restrict Drives"
policynameusb="Disable USB"
policynamecd="Disable CD-ROM"
policynameflpy="Disable Floppy"
policynamels120="Disable High Capacity Floppy"
explaintextusb="Disables the computers USB ports by disabling the usbstor.sys driver"
explaintextcd="Disables the computers CD-ROM Drive by disabling the cdrom.sys driver"
explaintextflpy="Disables the computers Floppy Drive by disabling the flpydisk.sys driver"
explaintextls120="Disables the computers High Capacity Floppy Drive by disabling the sfloppy.sys driver"
labeltextusb="Disable USB Ports"
labeltextcd="Disable CD-ROM Drive"
labeltextflpy="Disable Floppy Drive"
labeltextls120="Disable High Capacity Floppy Drive"
Enabled="Enabled"
Disabled="Disabled"
```

PŘÍLOHA P II: ADM SOUBOR PRO ZPŘÍSTUPNĚNÍ ZAKÁZÁNÍ JEN USB DISKŮ – DEFAULTNĚ ZAKÁZÁNO

```
CLASS MACHINE


CATEGORY "Services und Drivers"
    POLICY "USB Storage"
    KEYNAME "System\CurrentControlSet\Services\usbstor"
     PART "Startup type" DROPDOWNLIST
       VALUENAME "Start"
           ITEMLIST
           NAME "Boot" VALUE NUMERIC 0
           NAME "System"   VALUE NUMERIC 1
           NAME "Auto Load"   VALUE NUMERIC 2
           NAME "Load On Demand"       VALUE NUMERIC 3
           NAME "Disabled"   VALUE NUMERIC 4 DEFAULT
           END ITEMLIST
     END PART
    END POLICY
END CATEGORY
```

PŘÍLOHA P III: CD OBSAHUJÍCÍ ELEKTRONICKOU VERZI DIPLOMOVÉ PRÁCE A ZDROJOVÉ KÓDY SKENOVACÍHO SYSTÉMU