Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta

Katedra informatiky

Parametrizace Windows 7

Bakalářská práce

Petr Kofroň

Vedoucí práce

Ing. Václav Novák, CSc.

Rok 2011

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské/diplomové práce, a to v nezkrácené podobě pedagogickou fakultou elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích dne

Anotace

Tato bakalářská práce pojednává o nastavení operačního systému Windows 7 pomocí systémových registrů, zabývá se jejich funkcí, strukturou a významem. Seznamuje nás s programy a aplikacemi je spravující a uvádí konkrétní příklady editačních postupů. Je určena jako zdroj pro pochopení dané problematiky. Při použití této práce by měl být čtenář schopen nastavit parametry systému do jemu potřebné instance. Práce je primárně určena pro učitele na základní škole. Z toho vyplývá její záběr a koncept.

Abstract

This bachelor thesis is about the Windows 7 operating system settings by using the system registers. Deals with their function, structure and meaning.The text acquaints us with programs and applications which can be used to manage registr and show concrete examples of editing techniques. It's designed as a resource for understanding the Windows Registry. When you use this work, you should be able to set the system parameters to concrete value. The work is primarily intended for teachers at primary school. The scope and concept follows it.

Poděkování

Velice rád bych poděkoval panu Ing. Václavu Novákovi za pomoc s vedením práce.

Obsah

1 Úvod

Téma bakalářské práce jsem si zvolil pro zajímavý obsah a užitnou hodnotu. Při parametrizaci systému můžeme zvolit mnoho cest a způsobů, ale většina nastavení se stejně zapíše do systémového registru. Proto se mu v práci věnuji.

Na mnoho základních školách se používá starý operační systém Windows XP a z vlastních konzultací jsem vyrozuměl že v blízkém čase chtějí, nebo budou muset upgradovat na Windows 7. Proto práci cílím také na tuto skupinu.

Mnoho počítačově gramotných, pokročilých a zdatných laiků zná a ovládá systém a jeho četná nastavení a přizpůsobení, příliš ale nerozumí elegantnímu využívání registru. Tato práce to může změnit.

Vzhledem k zaměření na základní školy, kde je výskyt velkých sítí, nebo serverových řešení ojedinělý, tak toto téma nerozvíjím. Samostatně by vydalo na několik publikací.

Práce je rozdělena do několika částí. Nejdříve je vysvětleno co to je systémový registr a jeho struktura. Dále popisuje hodnoty a klíče registru. Hlavní klíče registru jsou detailně popsány.

Po vyrozumění s čím pracujeme se věnuji nástrojům s kterými můžeme data přímo editovat a následují příklady zápisu, exportu, importu a celých záloh. V dalších částech práci se věnuji složitějším procesům jako je sledování systému, nastavení systémového profilu atd.

Obsahem je také příklad pro demonstraci cíle a smyslu práce, závěr, obsah používané literatury a seznam zkratek a cizích slov použitých v práci.

Nastavení a úprava systémových registrů je zásahem do operačního systému. Proto je důležitá veliká opatrnost a uvědomění si prováděných změn.

2 Cíle práce

Cílem práce není konkrétní nastavení pracovní stanice, nýbrž představení možností jak toho dosáhnout. Aplikace postupů musí být univerzální pro libovolnou pracovní stanici s Windows 7.

Dokument by měl být srozumitelně formulován. Měl by zahrnovat možné postupy a situace, které využije učitel vyučující IT problematiku, nebo správce sítě na základní škole.

Při popisu registru se chci věnovat fyzické a logické struktuře. Zejména protože fyzická část je často v jiných publikacích opomíjena, nebo nedostatečně popsána. Důsledný popis věnuji i klíčům a hodnotám logické vrstvy.

Představená programová množina by pokud možno neměla zahrnovat placený a licencovaný software. Důvod je pragmatický – základní školy neoplývají četnými finanční prostředky.

Bakalářská práce bude prokládána praktickými příklady pro srozumitelnost obrazovými přílohami. Součástí by měl být i demonstrativní příklad. Při jeho řešení bude třeba znalostí z celého obsahu práce.

Bude přiložen seznam zkratek.

Cílem práce je vytvořit materiál umožňující pochopení parametrizace Windows 7.

3 Registry ve Windows 7

Registr systému Windows je hierarchická databáze, která ukládá konfigurační nastavení a možnosti operačního systému Microsoft Windows. Obsahuje nastavení pro nízko úrovňové systémové komponenty. Jako například pro aplikace běžící na platformách jádra, ovladačů zařízení, správce zabezpečení účtů, ale též i uživatelského rozhraní a aplikací třetích stran.

První systém využívající registry byly Windows 3.11. K většímu využití přišlo až s příchodem Windows 95. Registr nahrazuje soubory INI, které měly pro použití pro celý systém závažné nedostatky. Fyzicky je registr na disku uložen v několika souborech, tzv. „hives“, neboli podregistrech. Logicky potom do několika složek, nazývaných hlavními klíči. Neodborný, nebo nesprávný zásah do registrů může zapříčinit poškození registru a kritické důsledky pro funkčnost samotných Windows.

Výhodou oproti systému se soubory INI je to, že se údaje ukládají v binární podobě a umožňují víceuživatelské prostředí. Na jednom stroji pod jedním operačním systémem může tedy být více uživatelských profilů. Je možné tedy zavést pravidlo správcovského účtu. Tím získáváme i lepší zabezpečení proti možnému zborcení systému chybným zásahem, spuštění závadného programu či škodlivým softwarem.

Nevýhodou tohoto systému je paušálně nemožnost přenosu aplikací z počítače na počítač. Tím že programy zapíší do registru své nastavení a informace například o licencích, tak tyto data jsou pouze na jedné stanici. Přehráním programu na přenosné médium a spuštěním v jiném počítači se musí zapisovat znovu. Samozřejmě se to netýká edicí programů vytvořených přímo pro tyto účely.

3.1 Popis registrů a jejich funkce

3.1.1 Fyzická struktura registru

Fyzicky je databáze registru Windows uložena v různých souborech i adresářích na pevném disku. Jedná se o tzv. podregistry. V souborech podregistru jsou taktéž uložena nastavení k jednotlivým klíčům registru (ACL).

Tabulka s přehledem podregistrů – příloha č.1

3.1.2 Logická struktura registru

Registr obsahuje dva základní prvky: klíče a hodnoty.

3.1.2.1 Hodnoty

Hodnoty registru obsahují informace o názvu, typu a datech záznamu uloženého v klíči.

Každá hodnota může mít uložena libovolná data s proměnnou délkou a kódováním. Pro správnou analýzu musí mít definovaný typ, který reprezentuje. Každý typ má symbolický název pro lepší srozumitelnost.

Tabulka typů hodnot – příloha č.2

3.1.2.2 Klíče

Klíče registru jsou podobné složkám - kromě hodnoty klíče může každý obsahovat i podklíče, které mohou obsahovat další podklíče, a tak dále. Každý podklíč má povinný název, který je neprázdný řetězec, který nemůže obsahovat žádné lomítko nebo nulový znak.

Základní rozdělení je na pět soustav klíčů nazývaných hive(úl). Jejich názvy tedy začínají HKEY (*ukázkový obrázek* – příloha č.3) Hierarchie klíčů registru je přístupná pouze ze kořenového klíče, který je mapován na obsah klíče registru předem jádrem z uložených "úlů", nebo k obsahu podklíče v jiném kořenovém klíči. Může být také mapován na registrované služby nebo knihovnu DLL, která poskytuje přístup k jeho obsaženým podklíčům a hodnotám. Jednotlivé základní klíče se liší tím, jaké data nesou a zda jsou závislé na přihlášených uživatelích systému či nikoliv.

Klíče HKEY_LOCAL_MACHINE (globální nastavení systému) a KEY_CURRENT_USER (nastavení konkrétního přihlášeného uživatele) mají sobě podobnou strukturu. Uživatelská aplikace typicky zkontroluje svoje nastavení nejprve v KEY_CURRENT_USER a když ho nenalezne, prohledá stejnou hodnotu v stejném umístění v klíči HKEY_LOCAL_MACHINE.

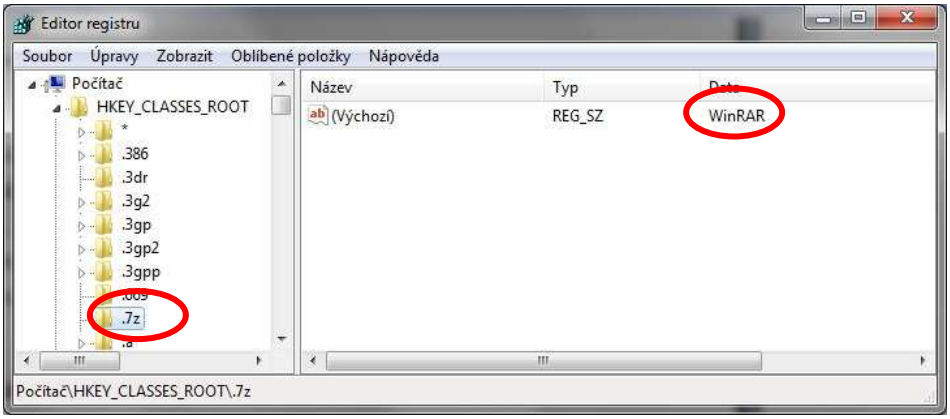
Klíče v registrech jsou zabezpečeny pomocí seznamu oprávnění (ACL) podobně jako je to mu souborového systému NTFS. Na hodnoty však nelze na rozdíl od klíčů aplikovat oprávnění ACL.

Ukázka nastavení okna ACL – příloha č.4

3.1.3 Popis základních klíčů registru

3.1.3.1 HKEY_CLASSES_ROOT

Obsahuje informace o registrovaných aplikacích, jako jsou asociace souborů a knihoven s jejich metodami. Klíč je propojen s HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES. Oba nesou stejná nastavení, ale přednost má tento.



Obrázek č.1 - Ukázka asociace souboru s příponou .7z s aplikací WinRAR.

3.1.3.2 HKEY_CURRENT_USER

Uchovává úplné nastavení přihlášeného uživatele. Obsahuje proměnné, nastavení plochy a vzhledu, mapování disku atd. Kompletně se to nazývá uživatelský profil. V systémech typu NT tedy i Windows 7 se nastavení uživatele v logické struktuře ukládá do souborů NTUSER.DAT a USRCLASS.DAT, ty jsou uloženy v profilové složce a jsou součástí

eventuálniho cestovního profilu mezi počítači. Tento propojen a generován s částí HKEY-USERS\S-(ID).

3.1.3.3 HKEY_LOCAL_MACHINE

Tento klíč ukládá nastavení, které jsou specifické pro konkrétní systém v místním počítači. Toto reprezentování klíče je virtuální. Klíč je udržován v paměti jádra systému mapováním ostatních klíčů a příslušných souborů z disku. Aplikace do něj nemohou přidávat další podklíče. Ve Windows Vista, Windows Server 2008, Windows Server 2008 R2 a Windows 7 je zastoupeno těchto 6 podklíčů – BCD, HARDWARE, SAM, SECURITY, SYSTEM a SOFTWARE.

3.1.3.3.1 BCD

Nese informace pro "bootování" systému.

3.1.3.3.2 HARDWARE

Je to nestálý a dynamicky generovaný klíč, není uložen v souboru. Obsahuje informace o aktuálně připojeném hardwaru a zařízeních Plug-n-Play.

Ukázka záznamu o procesoru počítače v programu regedit – příloha č.5

3.1.3.3.3 SYSTEM

Do tohoto klíče je možné zapisovat jen s udělenými administrátorskými právy pro přihlášeného uživatele na lokálním systému. Obsahuje data o nastavení systému, údaje týkající se generátoru čísel (RNG) a seznam aktuálně připojených zařízení se souborovým systémem. Očíslované podklíče "ControlSetXXX" obsahují platné a alternativní konfigurace pro ovladače hardwaru počítače, spuštěných služeb a nastavení Windows.

Klíč CurrentControlSet je dynamicky závislý na aktuálním "ControlSet" a sestavuje se při startu systému.

Každý ControlSet obsahuje podklíče:

"Enum" – Páruje všechny známé Plug-and-Play zařízení s nainstalovanými ovladači. Ukládá nastavení ovladačů.

"Services" – Klíč pro všechny ovladače s nespecifikovávaným nastavením, výčet zařízení kterým jsou instanciované a správu programů běžících jako služby.

"Control" – Tento klíč organizuje přístup běžících programů k ovladačům hardwaru.

"Policies" – Odkazovaný dynamický klíč vázaný k HKEY_LOCAL_MACHINE\SYSTEM\Software\Policies. Hlídá podmínky spouštění a provozu zařízení.

"Hardware Profiles" – Ukládá možné nastavení, nebo změny v jednotlivých profilech pro hardwarová zařízení počítače. Profily jsou buď v podklíčích "System" nebo "Software", protože úpravy se ukládají podle toho jestli je to defaultní profil systému, nastavení pro ovladače, nebo aplikací třetích stran. Také obsahuje číslované zálohy a současný/používaný profil.

Tyto dva klíče SAM a SECURITY jsou vidět jako prázdné. Slouží systému jako zástupci pro zabezpečovací politiku.

3.1.3.3.4 SAM

Slouží datům pojednávající o nastavení Správce zabezpečení účtů a domény, do kterých byl systém administrativně povolen, nebo nakonfigurován. Podklíče jsou tvořeny dle potřeby a odpovídají jeden každý pro doménu v nichž je systém.

3.1.3.3.5 SECURITY

Nastavuje zabezpečení přihlášeného uživatele v systému a doméně. Dynamicky je propojen s klíčem SAM.

3.1.3.4 HKEY_USERS

Klíč registru definující nastavení těch částí systému, které jsou závislé na profilu aktuálně přihlášeného uživatele.

Dělí se na tyto dva typy DEFAULT a S-(ID).

3.1.3.4.1 .DEFAULT

Výchozí profil nastavení systému před přihlášením jakéhokoliv uživatele. Všechny hodnoty jsou nastaveny jako při čerstvé instalaci Windows. Načítá se

pokud při zakládání nového profilu, nebo při přihlášení jako Quest (host). Tomu jen překopíruje hodnoty, ale nic se v něm nemění ani neukládá.

3.1.3.4.2 S-(ID)

Obsahuje profily všech uživatelů mající platný účet v systému. Název začíná písmenem S (session) a automaticky se vzestupně čísluje. Z tohoto klíče se generují hodnoty v HKEY_CURRENT_USER a HKEY_CURRENT_CONFIG.

3.1.3.5 HKEY_CURRENT_CONFIG

Tento klíč se také regeneruje při zavádění a běhu systému. Obsahuje konfigurace zapsané v hardwarových profilech. Váže se na "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current", který se ze začátku prázdný, ale při startu systému se naplní z "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles".

Díky tomuto principu je možné například přenosný počítač používat s různým hardwarem (třeba dokovací stanice).

3.2 Nástroje pro programovou manipulaci s registry

3.2.1 Editor registru "Regedit"

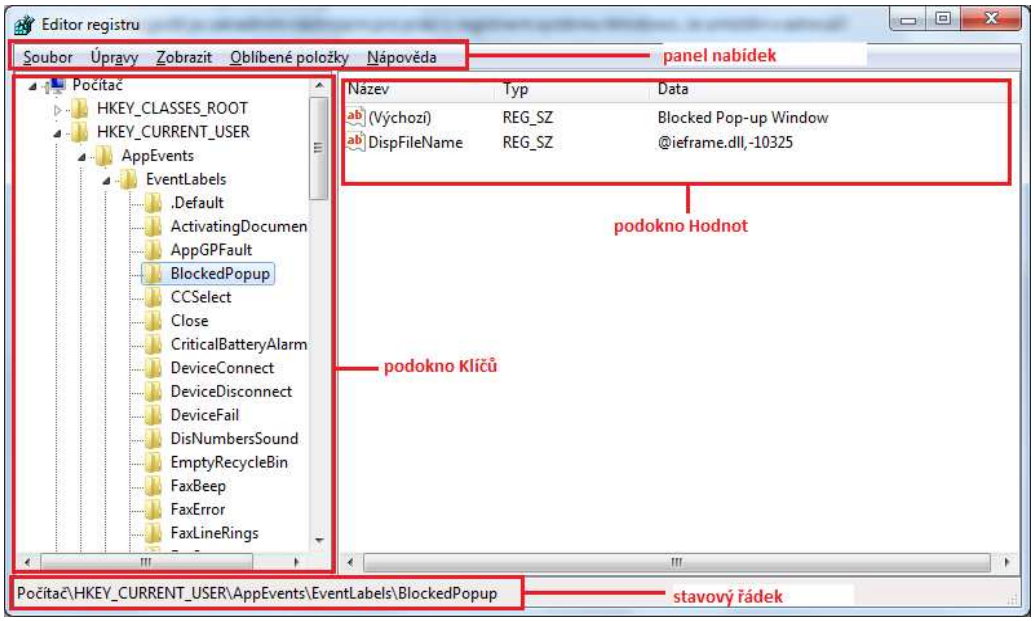
Regedit je základním nástrojem pro práci s registrem systému Windows. Je umístěn v adresáři %systemroot%, což je na většině PC adresář C:\Windows. Název spustitelného souboru je regedit.exe. V nabídce start není odkaz na spuštění Editoru registrů. Důvodem je, že není vhodné, aby běžní uživatelé bez vyšších znalostí registru, používali tento nástroj. Pomocí skupinových zásad, lze dokonce zabránit uživatelům ve spuštění nástroje regedit.

3.2.1.1 Spuštění nástroje Regedit

Klepněte na tlačítko "Start", potom na "Všechny programy - Příslušenství - Spustit ", v okně "Spustit" zadejte "regedit", a klepněte na "OK.

3.2.1.2 Grafické rozhraní

Editor registru je jednoduchý program s grafickým uživatelským rozhraním (GUI). Okno registru obsahuje v horní části menu, v dolní části stavový řádek. Střední, největší část okna je rozdělena na části. Vlevo jsou zobrazeny klíče, vpravo hodnoty. Práce s grafickým rozhraním je intuitivní a shodná s dalšími programy systému Windows.



Obrázek č.2 - Grafické rozhraní nástroje Regedit

3.2.1.2.1 Podokno klíčů

Zobrazuje hierarchickou strukturu registru. Na nejvyšší úrovni je položka Počítač reprezentující místní počítač. Pod touto položkou jsou základní klíče registru. Pod základními klíči se nacházejí další podklíče. Klíče lze sbalovat dvojklikem na klíč.

3.2.1.2.2 Podokno hodnot

Zobrazuje hodnoty aktuálně vybraného klíče. Hodnoty zobrazuje ve třech sloupcích „Název“, „TYP“, a „Data“. Šířku sloupců lze změnit dle potřeby.

3.2.1.3 Funkce nástroje Regedit

3.2.1.3.1 Úpravy registru

Úpravou registru rozumíme, vytváření, odstraňování, přejmenování, změna jednotlivých klíčů a hodnot. Používáme pokud chceme změnit chování operačního systému nebo aplikací.

3.2.1.3.2 Prohledávání registru

Důležitá funkce. Pokud například hledáme program který se spouští při každém spuštění systému Windows, můžeme příslušný klíč najít pomocí prohledávání registru na název hledaného programu.

3.2.1.3.3 Tisk registru

Nepříliš využívaná funkce. Umožňuje tisk části nebo celého registru.

3.2.1.3.4 Export a import registrů

Umožňuje ukládat celý registr nebo jeho část do souboru. Lze s výhodou použít, jako zálohu a obnovu při testování, nebo uložený registr použít později pro obnovení chování počítače do stavu v době exportu (zálohování).

3.2.2 REG.EXE

Nástroj pro práci s registry z příkazového řádku. Je alternativou ke grafickému nástroji Regedit. Je umístěn v adresáři %systemroot%\system32, název spustitelného souboru je REG.EXE. V zásadě vše co lze provést v grafickém nástroji Regedit, lze taktéž provést pomocí REG.EXE. Pomocí přepínačů lze provádět s registrem automatizované operace. Jedná se o nástroj bez uživatelského rozhraní. Jediným rozhraním jsou výstupy programu na obrazovku konzole programu CMD (interpreteru příkazů).

Náhled programu a možných příkazů – příloha č. 6

3.2.3 Powershell 2.0

V Powershellu je k dispozici Registry Provider, který umožňuje přístup ke klíčům registru, a k hodnotám. Registry Provider podporuje všechny cmdlety

obsahující sloveso „Item“ , jako jsou například Get-Item, Copy-Item, Rename-Item apod. Oprávnění ke klíčům je možno získávat pomocí Get-Acl.

Zajímavostí v Powershellu verze 2.0 je možnost provádět skupiny operací s registry v tzv. transakcích (dosud známých pouze z databázových systémů). Skupina operací s registry tzv. transakce se zahajuje příkazem Start-Transaction. Poté následuje skupina operací s registry s parametrem –useTransaction. Pokud se všechny operace provedou bez chyb, je nakonec transakce potvrzena příkazem Complete-Transaction a změny jsou zapsány do registru. V případě, že byť jediná operace uvnitř transakce skončí chybou, potom je proveden tzv. Roll-back transakce kdy není provedena žádná operace uvnitř transakce. Transakce tedy zaručuje, že buď budou provedeny všechny operace uvnitř transakce, nebo žádná.

Příklad použití transakcí:

```
Start-Transaction

New-Item -type directory -path hkcu:\test -UseTransaction

New-ItemProperty -path HKCU:\Test -name Hodnota1 -value
"Test transakcí." -useTransaction

New-ItemProperty -path HKCU:\Test -name Hodnota2 -value
"Test transakcí." -useTransaction
Complete-Transaction
```

3.3 Formy zápisu do registru

3.3.1 Přístup a editace

Formy zápisu klíčů a hodnot do registrů se liší v závislosti na použitém nástroji nebo metodě přístupu. Níže uvedené jsou zápisy jednotlivých typů hodnot v nástrojích Regedit, Reg a „REG“souboru.

3.3.1.1 Řetězcová hodnota – REG_SZ

3.3.1.1.1 Zápis v nástroji Regedit:

Do dialogového okna „Upravit řetězec“ napíšeme požadovanou hodnotu.

3.3.1.1.2 Zápis v REG souboru:

Hodnotu typu řetězec píšeme do uvozovek.

Příklad zápisu:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Hodnoty]
"řetězcová hodnota"="příklad řetězcové hodnoty"
```

3.3.1.1.3 Zápis z příkazové řádky:

Hodnotu typu řetězec píšeme do uvozovek.

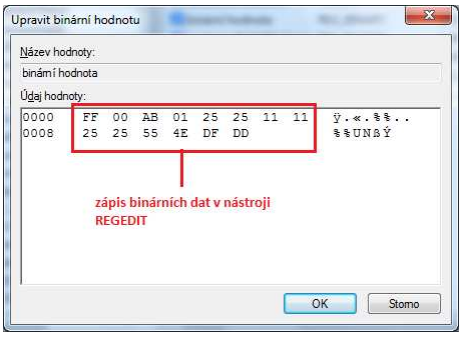
Příklad zápisu:

```
C:\Windows\System32> reg add HKCU\Hodnoty /v "řetězcová
hodnota" /t REG_SZ /d "název řetězcové hodnoty" /f
```

3.3.1.2 Binární hodnota – REG_BINARY

3.3.1.2.1 Zápis v nástroji Regedit

Binární data zapisujeme pomocí šestnáctkového zápisu.



Obrázek č.3 - zápis binární hodnoty

3.3.1.2.2 Zápis v REG souboru

Hodnoty zapisujeme „hex:“ následované hodnotami v šestnáctkovém formátu oddělené čárkami.

Příklad zápisu:

```
[HKEY_CURRENT_USER\Hodnoty]
"binární hodnota"=hex:a0,01,fa,ef,ff,25,20,22,50,02,01,…
```

3.3.1.2.3 Zápis z příkazové řádky:

Binární data zapisujeme v šestnáctkovém formátu najednou bez mezer.

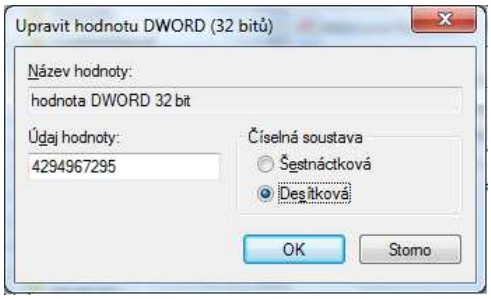
Příklad zápisu:

```
C:\Windows\System32> reg add HKCU\Hodnoty /v "binární
hodnota" /t REG_BINARY /d
  a001faefff25202250020111dd001110 /f
```

3.3.1.3 Hodnota DWORD (32 bitů) – REG_DWORD

3.3.1.3.1 Zápis v nástroji Regedit

Čtyřbajtové hodnoty se zobrazují a upravují v desítkovém nebo šestnáctkovém formátu.



Obrázek č.4 - zápis čísla do registru pomocí regedit-u

3.3.1.3.2 Zápis v REG souboru

Hodnoty zapisujeme „dword:“ následované hodnotou v šestnáctkovém formátu.

Příklad zápisu:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Hodnoty]
"hodnota DWORD 32 bit"=dword:ffffffff
```

3.3.1.3.3 Zápis z příkazové řádky

DWORD 32bitů zapisujeme v desítkovém formátu.

Příklad zápisu hodnoty `4294967295` :

```
C:\Windows\System32> reg add HKCU\Hodnoty /v "hodnota
DWORD 32 bit" /t REG_DWORD
 /d 4294967295 /f
```

3.3.1.4 Hodnota DWORD (64 bitů) – REG_QWORD

3.3.1.4.1 Zápis v nástroji Regedit:

Osmi bajtové hodnoty se zapisují a upravují v desítkovém nebo šestnáctkovém formátu.

3.3.1.4.2 Zápis v REG souboru:

Hodnoty zapisujeme „hex(b):“ následované hodnotami v šestnáctkovém formátu oddělené čárkami.

Příklad zápisu:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Hodnoty]
"hodnota DWORD 64bit"=hex(b):ff,ff,ff,ff,ff,ff,ff,ff
```

3.3.1.4.3 Zápis z příkazové řádky:

DWORD 64bitů zapisujeme v desítkovém formátu.

Příklad zápisu hodnoty `18446744073709551615` :

```
C:\Windows\System32> reg add HKCU\Hodnoty /v "hodnota
DWORD 64bit" /t REG_QWORD
/d 18446744073709551615 /f
```

3.3.1.5 Víceřetězcová hodnota – REG_MULTI_SZ

3.3.1.5.1 Zápis v nástroji Regedit:

Jednotlivé řetězce se zapisují v řádcích pod sebou.

3.3.1.5.2 Zápis v REG souboru:

Hodnoty zapisujeme „hex(7):“ následované hodnotami v šestnáctkovém formátu oddělené čárkami. Jednotlivé řetězce odděluje znak 0x00, seznam řetězců ukončují dva znaky 0x00.

Příklad zápisu:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Hodnoty]
"víceřetězcová
hodnota"=hex(7):31,00,31,00,31,00,31,00,31,00,00,00,32,00
,32,00,…\
```

3.3.1.5.3 Zápis z příkazové řádky:

Jednotlivé řetězce oddělujeme znaky `\0`. Pokud všechny řetězce uzavřeme do uvozovek, můžeme v řetězcích používat mezery.

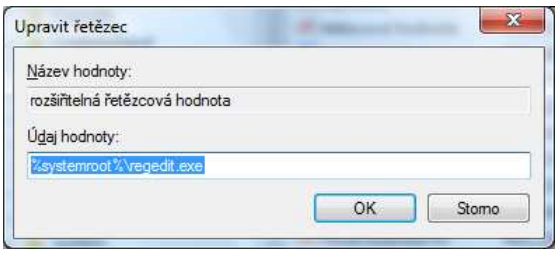
Příklad zápisu:

```
C:\Windows\System32> reg add HKCU\Hodnoty /v
"víceřetězcová hodnota" /t REG_MULTI_SZ /d
"11111\022222\033333\0abcde" /f
```

3.3.1.6 Rozšiřitelná řetězcová hodnota

3.3.1.6.1 Zápis v nástroji Regedit:

Hodnoty zadáváme stejně jako u řetězcové hodnoty REG_SZ, proměnné zapisujeme ve formátu %názevproměnné%.



Obrázek č.5 - zápis hodnoty v regedit-u

3.3.1.6.2 Zápis v REG souboru:

Hodnoty zapisujeme „hex(2):“ následované hodnotami v šestnáctkovém formátu oddělené čárkami.

3.4 Zálohování registru

Podobně jako u editace jednotlivých hodnot a klíčů, i při zálohování registrů lze použít různé metody.

3.4.1 Zálohování a obnova registrů pomocí REG souborů

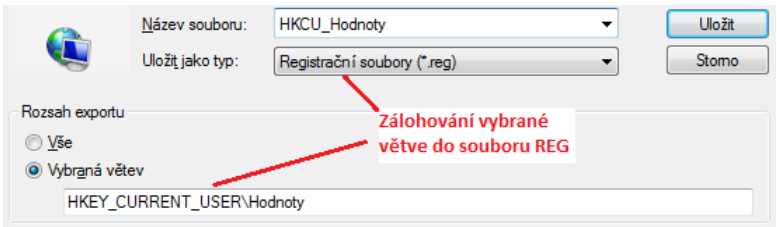
Nástroj Regedit i REG.EXE umožňuje exportovat (zálohovat) vybranou větev do souboru typu REG. Soubor má snadno čitelný textový obsah, a je upravitelný v libovolném textovém editoru. Pro svoji snadnou čitelnost je vhodný taktéž pro dokumentaci úprav v registrech.

V případě použití REG souboru pro import (obnovení) je důležité si uvědomit, jakým způsobem import probíhá. Jedná se o tzv. merge metodu, kdy je registr pouze aktualizován podle REG souboru, a ostatní hodnoty v REG souboru neuvedené jsou ponechány v systému. Z těchto důvodů není exportování do REG souboru vhodné pro zálohování celých větví registru. Lze ji však doporučit pro zálohování konkrétních nastavení, nebo pro aplikaci konkrétních nastavení .

Ukázka obsahu REG souboru – příloha č.7

3.4.1.1 Zálohování v nástroji Regedit:

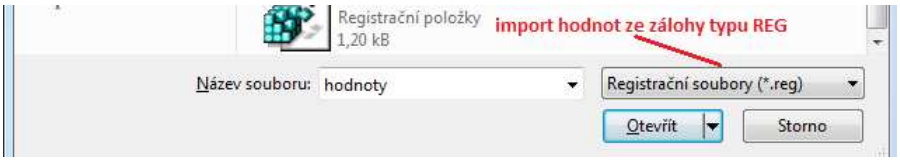
1. v podokně klíčů označíme klíč, který chceme zálohovat
2. v menu „Soubor“ klepneme na položku „Exportovat“.
3. V okně „exportovat soubor registru“ uložit typ souboru jako „Registrační soubory (*.reg)“
4. Kliknout na uložit.



Obrázek č.6 - zálohování klíče

3.4.1.2 Obnova v nástroji Regedit:

1. V programu Regedit v menu „Soubor“ klepneme na položku „Importovat“
2. V okně „Importovat soubor registru“ vybereme typ souboru „Registrační soubory (*.reg)“, následně vybereme příslušný reg soubor, a klikneme na otevřít.



Obrázek č.7 - Import klíče

3.4.1.3 Zálohování v nástroji REG.EXE

1. V příkazovém řádku zadáme příkaz REG EXPORT

Příklad zápisu:

```
reg export HKCU\Hodnoty C:\users\test\hodnoty.reg /y
```

3.4.1.4 Obnova v nástroji REG.EXE

1. V příkazovém řádku zadáme příkaz REG IMPORT

Příklad zápisu:

```
C:\Windows\System32>reg import c:\users\test\hodnoty.reg
```

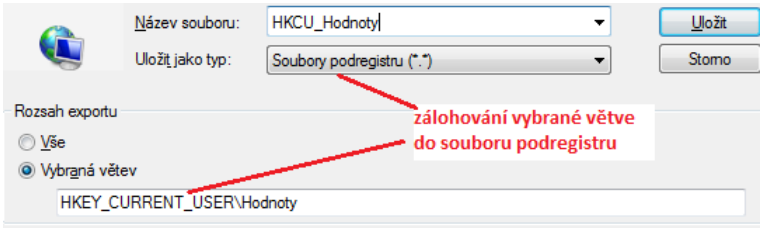
3.4.2 Zálohování a obnova registrů pomocí souborů podregistrů

Další možností, jak zálohovat a obnovovat větve registrů je tzv. soubor podregistru. Jedná se často opomíjenou a méně známou metodu práce s registrem. Soubor podregistru je binární soubor který obsahuje část registru (větev). Tento soubor není čitelný v textovém editoru, protože je uložen nativním formátu registru Windows. Na rozdíl od souborů typu REG, při importu souboru typu podregistr, je importovaná větev včetně všech vnořených

klíčů a hodnot nejdřív odstraněna, a poté obnovena ze souboru. Lze ji tedy doporučit pro vytváření záloh celých větví registru. Nevýhodou použití této metody je nemožnost editace v textovém editoru, naopak výhodou, je možnost soubor připojit a modifikovat prostřednictvím nástroje Regedit.

3.4.2.1.1 Zálohování v nástroji Regedit:

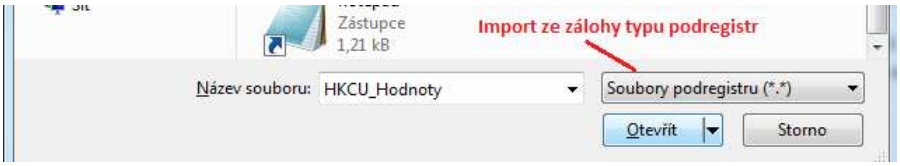
1. V podokně klíčů označíme klíč, který chceme zálohovat
2. V menu „Soubor“ klepneme na položku „Exportovat“.
3. V okně „exportovat soubor registru“ uložit typ souboru jako „Soubory podregistru“
4. Kliknout na uložit.



Obrázek č.8 - Záloha podregistrů

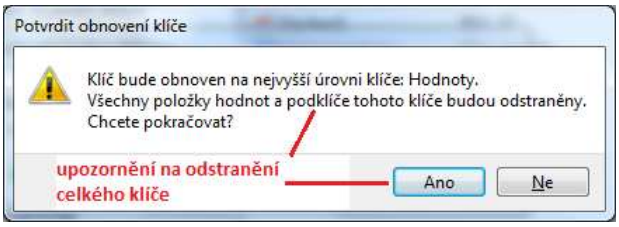
3.4.2.1.2 Obnova v nástroji Regedit:

1. V menu „Soubor“ klepneme na položku „Importovat“
2. V okně „Importovat soubor registru“ vybereme typ souboru „Soubory podregistru“, následně vybereme příslušný soubor, a klikneme na otevřít.



Obrázek č.9 - Záloha podregistru

3. V okně „Potvrdit obnovení klíče“ klepněte na „Ano“. Uvedený klíč bude před obnovením smazán.



Obrázek č.10 - Varovné upozornění při obnově podregistru

3.4.2.1.3 Zálohování v nástroji Reg.exe:

1. Pro zálohování zadáme příslušný příkaz REG SAVE

Příklad zápisu:

```
reg save HKCU\Hodnoty c:\users\test\hodnoty /y
```

3.4.2.1.4 Obnova v nástroji Reg.exe:

1. Pro obnovu zadáme příslušný příkaz REG RESTORE

Příklad zápisu:

```
reg restore HKCU\Hodnoty c:\users\test\hodnoty
```

3.4.3 Použití funkce Obnovení systému

Od systému Windows XP je možné použít pro zálohování registru systému vestavěný nástroj „Obnovení systému“. Tento nástroj sleduje změny v operačním systému a aplikacích a na základě těchto změn vytváří tzv. body obnovení. Protože součástí bodu obnovení je mimo jiné záloha všech souborů podregistrů, je možné funkci využít k záloze a obnově celého registru. Nápověda pro používání nástroje je součástí systému.

3.4.4 Zálohování registrů off-line pomocí Windows PE

Předchozí způsoby zálohování a obnovy registrů vyžadují, aby obnovovaný operační systém byl spuštěný – tedy ve stavu on-line. V okamžiku kdy víme kam operační systém soubory podregistrů ukládá, můžeme je zálohovat i ve stavu off-line. Od systému Windows Vista je nejjednodušším způsobem pro zálohování registrů off-line použití bootovatelného Windows Preinstallation Environment (Windows PE) média. Windows PE je prostředí určené pro instalaci, diagnostiku, zálohování a řešení problémů. Lze jej získat zdarma stažením balíčku WAIK (Windows Automated Installation Kit). Uvedený

balíček obsahuje „step-by-step“ návody pro vytvoření bootovatelných PE médií.

3.4.4.1.1 Záloha registrů pomocí Windows PE

1. Na počítači, na kterém chceme provést zálohu registrů, spustíme prostředí Windows PE.
2. V prostředí příkazové řádky zadáme příslušný příkaz pro zkopírování (zálohu) souboru podregistru.

```
x:\xcopy d:\windows\system32\config\system e:\zaloha
\system.hiv
```

3. Pro ukončení práce s Windows PE zadáme příkaz pro restart systému.

```
wpeutil reboot
```

3.4.4.1.2 Obnova registrů pomocí Windows PE

1. Na počítači, na kterém chceme provést obnovu registrů, spustíme prostředí WindowsPE.
2. V prostředí příkazové řádky zadáme příslušný příkaz pro zkopírování (obnovu) souboru podregistru.

```
x:\xcopy e:\zaloha\system.hiv
d:\windows\system32\config\system
```

3. Pro ukončení práce s Windows PE zadáme příkaz.

```
wpeutil reboot
```

4 Použití registrů při běhu programu

Základem používání registru k ovlivňování chodu systému nebo aplikací, je znalost kdy a jak systém nebo aplikace registr používá. U některých aplikací postačí spustit import reg souboru po přihlášení uživatele, jiná aplikace si vyžádá editaci registru off-line (např. reset hesla administrátora PC).

4.1 Získání znalostí o chování programu

4.1.1 Referenční příručka k nastavení skupinových zásad

V systému Windows je grafický nástroj „Editor místních zásad skupiny“, který grafickým rozhraním umožňuje ovlivňovat chování systému Windows a jeho aplikací. K tomuto nástroji je k dispozici Referenční příručka k nastavení skupinových zásad. V této příručce je uvedeno přes 3000 nastavení, které lze nastavit pomocí šablon zabezpečení skupinových zásad.

Na internetu je příručka ke stažení pod názvem „Group Policy Settings Reference for Windows and Windows Server“. Také jí je možné procházet online na internetu.

Odkazy ke stažení a prohlížení – příloha č.8

4.1.2 Windows Server 2003 Resource Kit Registry Reference

On-line je k dispozici referenční příručka k systému Windows Server 2003, která obsahuje detailní informace k vybraným klíčům operačního systému.

Odkazy k prohlížení – příloha č.8

4.1.3 Dokumentace k instalovanému software

V dokumentaci nebo instalační příručce lze často najít důležité informace o tom, jak programové vybavení nainstalovat a přizpůsobit.

4.1.4 Prohledávání registru

Pokud nemáme k dispozici potřebnou dokumentaci nebo SW. Můžeme v některých případech použít metodu prohledávání registru. Typickým příkladem použití, je vyhledání autospouštění programů po startu systému.

4.1.5 Monitorování registru za běhu programu

K zjištění informací, jakým způsobem program zapisuje do registrů, můžeme využít programy pro sledování zápisu do registrů.

5 Manipulace s registry pro administrátory na ZŠ

5.1 Programy a aplikace

Výrobce operačního systému Windows uvádí, že není obvykle nutné provádět přímé úpravy registru. Přímou úpravou jsou myšleny tzv. nízko-úrovňové nástroje typu Regedit, Reg, a další. Pokud tedy je k dispozici jiná metoda vyšší úrovně, či metoda k danému úkolu přímo určená, je vhodné jí použít. Většinou je vhodné použít nástroj přímo dodávaný výrobcem software, než nástroje třetích stran.

5.1.1 Zásady skupiny „Group Policy“

Jsou vhodným nástrojem pro manipulaci s registrem, pokud spravovaný počítač je členem domény Windows. Pomocí zásad skupiny lze spravovat nastavení týkající se registru HKEY_LOCAL_MACHINE (nastavení počítače), i nastavení týkající se registru HKEY_CURRENT_USER (nastavení uživatele). Vytvořená nastavení lze aplikovat na skupiny počítačů nebo uživatelů podle požadavku školy. Lze tedy snadno vytvořit stejné prostředí pro všechny počítače ve třídách.

5.1.2 Nástroje pro úpravu registru dodané výrobcem SW

Výrobce konkrétního programu často dodává nástroje pro přizpůsobení. Výhodou těchto nástrojů je nemalá úspora času a problémů které nám můžou ušetřit. Obsahují grafické rozhraní a kontrolu syntaktické správnosti zápisu.

Příklady nástrojů pro přizpůsobení instalace:

- Custom Installation Wizard - Office 2003 Resource Kit – Odkaz na stažení – Příloha.9
- Customization Tool in the 2007 Office – Je přímo součástí instalace balíku Office . Odkaz na stažení – Příloha.9
- Office Customization Tool in Office 2010 – Je přímo součástí instalace balíku Office. Odkaz na stažení – Příloha.9
- Internet Explorer Administration Kit (IEAK)
  Odkaz na stažení – Příloha.9
- Adobe Customization Wizard X – Pro přizpůsobení instalace Adobe Reader . Odkaz na stažení – Příloha.9

5.1.3 Nástroje pro přizpůsobení a automatizaci instalace operačního systému

Od Windows Vista byl kompletně přepracován způsob instalace operačního systému. Jednou z hlavních změn je fakt, že celá instalace je uložena v jednom souboru tzv. image. Tento image je při instalaci aplikován (rozbalen) na pevný disk počítače. Spolu s nástroji nám to přináší možnosti, jak ušetřit čas s instalací a nastavením operačního systému. Přiblížení přizpůsobení jednotlivých nástrojů by bylo obsahem na celou další práci, proto se jimi nebudu zabývat podrobně.

Nástroje pro přizpůsobení instalace operačního systému:

- Windows Automated Installation Kit - Odkaz na stažení – Příloha.10
- Microsoft Deployment Toolkit – Odkaz na stažení – Příloha.10

5.1.4 Nástroj pro User State Migration Tool

V případě reinstalace nebo instalace nového počítače, je jedním z úkolů přenesení uživatelských a některých systémových nastavení. S tímto úkolem nám může pomoci nástroj USMT, který je určený pro zálohování, obnovu, nebo přesun (migraci) uživatelských profilů.

USMT pracuje se soubory XML, které je možné upravit, případně doplnit o námi požadovaná nastavení, nebo aplikace. XML soubory je taktéž možné využít ke studiu.

Výběr nastavení založených na registru, která můžeme aplikovat pomocí USMT:

- Ovládací panely: Možnosti usnadnění, možnosti složky, myš, klávesnice, místní a jazykové nastavení, spořič obrazovky, zvuky a zvuková zařízení, hlavní panel a nabídka start
- Nastavení příkazové řádky
- Nastavení Windows Media player
- Nastavení Microsoft Internet Explorer
- Nastavení některých dalších aplikací. Např. IBM Lotus Notes, Adobe Acrobat Reader, Microsoft Office, a další.

Odkaz na stažení – Příloha.10

5.1.5 Úpravy registrů off-line pomocí Windows PE média

V okamžiku kdy registry nemůžeme upravovat on-line, tedy přímo ze spuštěného operačního systému, můžeme použít bootovatelného Windows PE média ke spuštění prostředí Windows PE. Z prostředí Windows PE máme soubory pod-registru k dispozici off-line a můžeme si je přenést na jiný počítač se systémem Windows 7. V tomto počítači pak připojíme soubor pod-registru do nástroje Regedit, v něm provedeme patřičné změny. Opravený soubor pod-registru pak vrátíme do původního počítače.

5.1.6 Úpravy registrů off-line, pomocí speciálních bootovatelných médií

Mezi tyto nástroje patří např. Off-line NT Password & Recovery editor, který umožňuje off-line editovat soubor pod-registru SAM z pevného disku počítače, kde jsou uloženy hesla uživatelů a další nastavení zabezpečení.

Odkaz na stažení – Příloha.10

5.1.7 Nástroj Process Monitor

Tento nástroj umožňuje v reálném čase monitorovat aktivitu procesů, jejich zápis na pevný disk, zápisy do registrů a další.

Odkaz na stažení – Příloha.10

5.1.8 Nástroj Autoruns for Windows

Tento nástroj dokáže zobrazit seznam všech programů, které se spouštějí automaticky po spuštění Windows. Nejspíš je to nástroj s nejobsáhlejší databází tohoto typu. Je vhodný i pro studium registru.

Odkaz na stažení – Příloha.10

5.2 Specifika prostředí v učebnách na ZŠ

Prostředí v učebnách ZŠ a vůbec ve školách má svá specifika. Základním požadavkem bývá kromě funkčnosti aplikačního software, požadavek na stejné nastavení prostředí operačního systému a aplikací. V následujících odstavcích jsou hlavní specifika popsány podrobněji.

5.2.1 Různé hardwarové vybavení

V jedné počítačové učebně jsou často počítače různé výkonnosti, a odlišného hardwarového vybavení. Toto vyžaduje instalaci odlišných operačních systémů, ovladačů, nebo aplikačního software. Sjednotit takové prostředí může být značně problematické.

5.2.1.1 Odlišnost operačních systémů v rámci učebny

Mezi Windows XP a Windows 7 jsou z uživatelského pohledu velké rozdíly. Je sice možnost systém Windows 7 přizpůsobit tak, aby vypadal podobně jako Windows 7, myslím ale, že to není z hlediska výuky vhodné. Výhodné je v rámci učebny soustředit výkonově podobné počítače, aby bylo možné na všech nainstalovat stejný operační systém.

5.2.1.2 Odlišnost a kvalita hardwarového vybavení v rámci učebny

Daleko obtížněji lze dosáhnout stejného hardwarového vybavení na všech počítačích v rámci učebny, nebo všech učeben. Školy nejsou banky, aby měly finanční prostředky na kompletní výměnu počítačů jednou za 3 roky. Při výběru HW je tedy třeba brát v úvahu nejenom výkon nakupovaného PC, ale i záruku, podporu a zabezpečení. Škola by si měla určit svoje standardy pro nákup PC, a ty dodržovat.

5.2.1.3 Možnosti řešení

- Kvalitní záruka – může například zajistit výměnu za stejný hardware po dobu záruky
- Podpora – ovladače pro operační systém v nativním formátu systému Windows. Usnadní instalaci operačního systému z jedné instalace na různý hardware

5.2.2 Uvedení nastavení programu do původního stavu

Programy v dnešní době obsahují spousty různých nastavení a přizpůsobení. Uživatel si tak může program přizpůsobit pro vlastní potřebu, aby program používal co nejefektivněji. Toto chování ale může způsobovat problém ve výuce, když učitel potřebuje, aby program byl ve výchozím nastavení. Někdy

je zase výše uvedené chování žádoucí, pokud žáci již program znají a chtějí program využívat efektivně. V těchto případech je výhodné použít některé metody

5.2.2.1 Příklady možností řešení

- Rychlá obnova počítače do původního stavu -
    - Obnova z image uloženého na pevném disku počítače
- Obnovení původních hodnot nastavení v registru
    - Např. po přihlášení uživatele může být spuštěn skript, který automaticky obnoví příslušná nastavení

5.2.3 Zabezpečení počítače při výuce

Jedním z úkolů správců sítí je zabezpečení chodu počítačů ve škole. Běžný žák by neměl mít možnost startovat z USB klíče nebo optické mechaniky vlastní nástroje nebo operační systém. Taktéž by žák neměl mít možnost měnit nastavení operačního systému, instalovat aplikace apod.

5.2.3.1 Řešení

- Zákaz startu operačního systému z vyměnitelného média. Zabezpečuje se na úrovni systému BIOS. Tuto možnost by měl mít k dispozici pouze správce učebny.
- Žák by měl být přihlášen s oprávněními běžného uživatele. Tím je zabráněno nežádoucím změnám v operačním systému a aplikacích.
- Řešením mohou být i programy třetích stran pro ochranu nebo obnovení změn v registrech.

5.2.4 Zabezpečení počítače při zkoušení žáků

Při zkoušení žáků může být potřeba zajistit specifické prostředí. Může to být zákaz spuštění nežádoucích programů, zákaz připojení vyměnitelných médií, externích disků, zákaz prohledávání internetových stránek apod.

5.2.4.1 Možnosti řešení

- Kombinace různých metod zabezpečení na bázi registrů.

- Vytvoření odděleného image operačního systému určeného pro zkoušení.

5.2.5 Problematika virů a spyware

Doporučením je samozřejmě používat aktualizovaný antivirový software. V některých případech se znalost registru může hodit pro odstranění nežádoucích programů při spuštění počítače, nebo k tomu využít utilitu k tomu určenou např. „Autoruns for Windows“ dostupnou ke stažení.

5.2.6 Zabránění automatického spuštění z vyměnitelných disků

Viry se dnes šíří nejen po internetu, ale i po vyměnitelných zapisovatelných médiích, a využívají k tomu funkci automatického spuštění z vyměnitelného média. Řešením může být vypnutí funkce „spustit automaticky“ prostřednictvím registrů.

5.3 Shrnutí základních požadavků na manipulaci s registry

Požadavky na manipulaci s registry se mohou značně lišit v závislosti na zadání nebo použitých nástrojích. V každém případě bychom měli vždy důkladné prostudovat typ klíče a změny kterou chceme provést.

Příklady:

- Uživatel musí rozumět problematice.
- Pro editaci musíme mít přidělenou adekvátní ACL.
- Doporučuji provádět zálohu před zapsáním hodnot.
- Zapisovat jen do klíčů kterým rozumíme a víme co změnou způsobíme.
- Pro učební a testovací účely je vhodné používat virtuální stroj – příloha č.12.
- Při hledání řešení je vhodné využít online či offline příručky .
- Pro editace velkých částí a zálohy je lepší využít jiného programového prostředku než regedit, nebo REG.EXE.

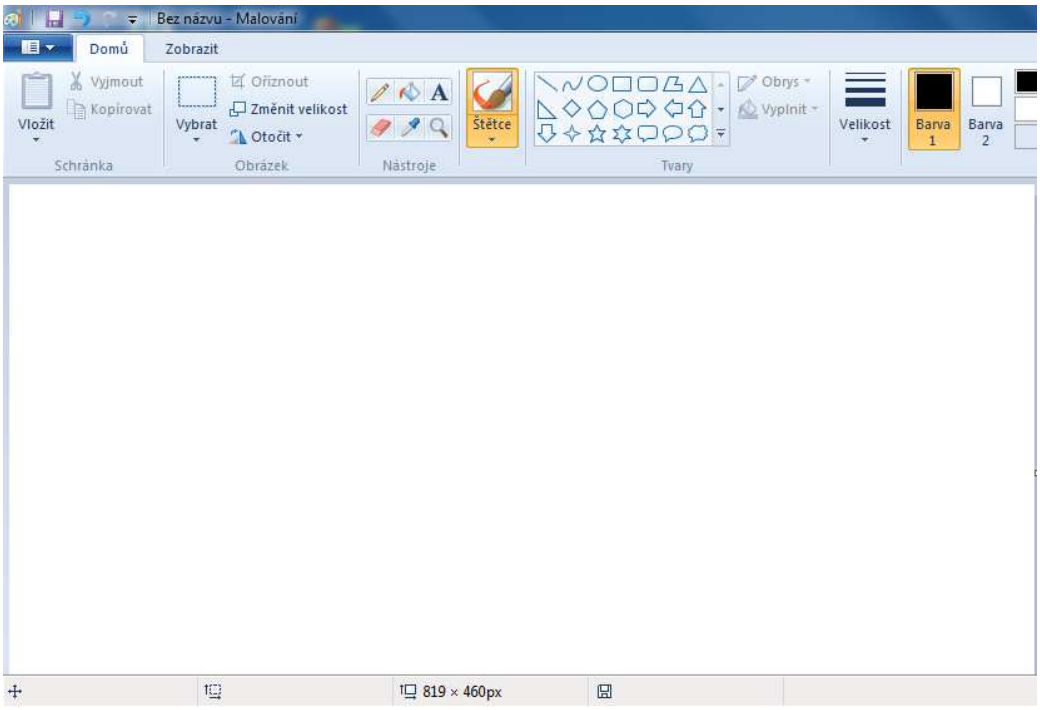
- Editace přímo v souboru REG je výhodná pouze při elementárních úkonech.
- Pro dávkové změny se hodí použití PowerSheell 2
- Vhodnou úpravou uživatelských práv omezíme možnost editace našich nastavení jinými osobami.
- Pro správu více PC je vhodné využívat například “Zásady skupiny“ a programy pro migraci uživatelů.

6 Demonstrativní příklad

6.1 Malování

6.1.1 Zadání

Předpokládejme následující scénář. Na počítači s operačním systémem Windows 7 Professional chceme zajistit, aby po přihlášení uživatele bylo vždy nastavení programu Malování ve výchozím stavu. To znamená, že bude program Malování spuštěn v maximalizovaném okně, a pás karet nebude minimalizovaný. Program tak bude připravený vždy pro výuku.

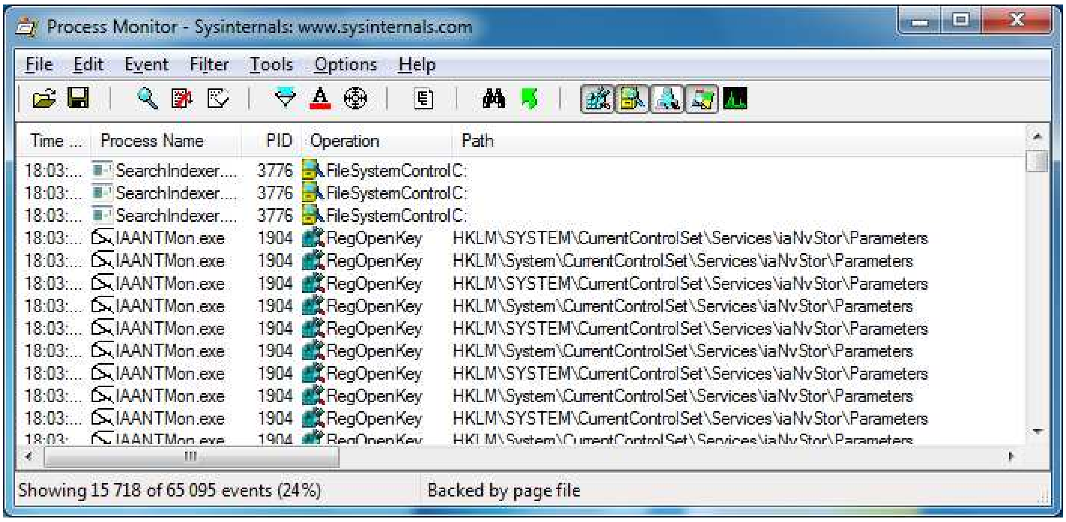


Obrázek č.11 - Základní nastavení programu malování

6.1.2 Postup

6.1.2.1 Spuštění programu Process Monitor.

Z pevného disku přímo spustíme soubor Procmon.exe. Na obrázku č.12 je vidět spuštěný Process Monitor ve výchozím nastavení kdy monitoruje aktivitu všech procesů.



Obrázek č.12 - Program Process Monitor

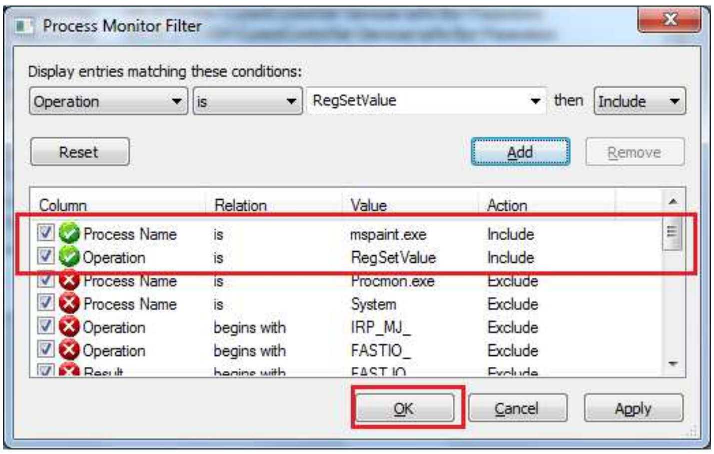
6.1.2.2 Nastavení filtru procesů.

a. V menu Process Monitoru klikneme na „Filter“ a v podmenu klepneme na „Filter“. Zobrazí se dialogové okno „Process Monitor Filter“.

b. V okně „Process Monitor Filter“ klepneme na tlačítko „Reset“. Tím smažeme případný již nastavený filtr.

c. Přidáme filtr pro jméno procesu. V horní části okna „Process Monitor Filter“ nastavíme podmínku pro zachycení aktivity. „Process Name is mspaint.exe“ then „Include“ a pak klikneme na tlačítko „Add“

d. Přidáme filtr pro operaci. V horní části okna „Process Monitor Filter“ nastavíme podmínku pro zachycení aktivity. „Operation is RegSetValue“ then „Include“ a pak klikneme na tlačítko „Add“. Na závěr zkontrolujeme nastavení (viz. Obrázek č.13) a klikneme na tlačítko „Ok“.

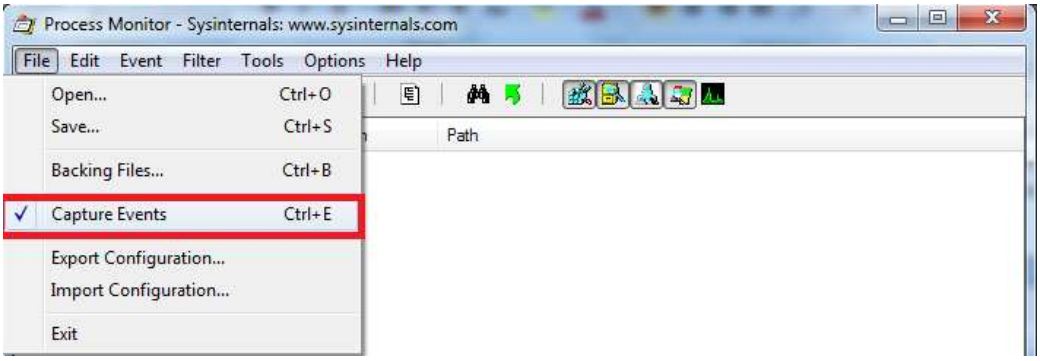


Obrázek č.13 - Nastavení filtru pro zachycení aktivity

6.1.2.3 Zapnutí záznamu událostí

V okně Process Monitor klepneme v menu „Edit“ na položku „Clear display“. Dále zkontrolujeme zaškrtnutí položky v menu „File“ – „Capture Events“

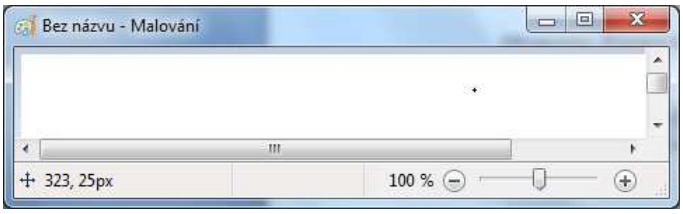
Obrazovka „Process Monitoru“ by měla vypadat následovně:



Obrázek č.14 - Zaškrtnutí záznamu událostí

6.1.2.4 Spuštění programu „Malování“.

a. V programu minimalizujeme Pás karet tím, že klikneme na Pás karet pravým tlačítkem myši, a klikneme na „Minimalizovat pás karet“.
b. Zmenšíme velikost okna malování (viz. Obrázek č.15)



Obrázek č.15 - Zmenšené okno programu

c. Ukončíme program Malování a poznamenáme si aktuální čas. V této ukázce to bylo v 18:40

6.1.2.5 Nastavení vzhledu

a. Počkáme několik minut, a znovu spustíme program „Malování“

b. Maximalizujeme okno „Malování“.

c. Zrušíme minimalizaci pásu karet.

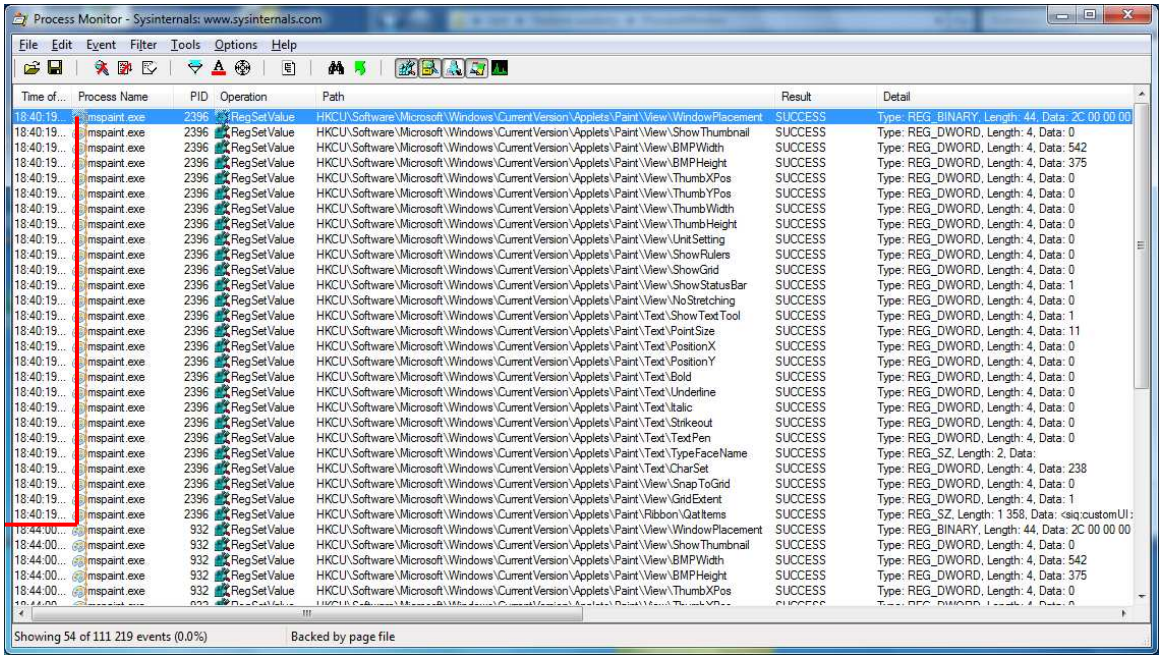
d. Ukončíme program Malování a poznamenáme si aktuální čas. V této ukázce to bylo v 18:44

6.1.2.6 Analýza

d. Přepneme se zpět do okna Process Monitoru.

e. Zrušíme zaškrtnutí položky v menu „File“ – „Capture Events“

f. Provedeme analýzu zachycených událostí zápisu. Z výpisu je patrné, že program Malování zapisuje do registrů vždy při ukončení programu. Prvních 27 zachycených událostí zápisu do registru je v 18:40, dalších 27 událostí zápisu je v 18:44.

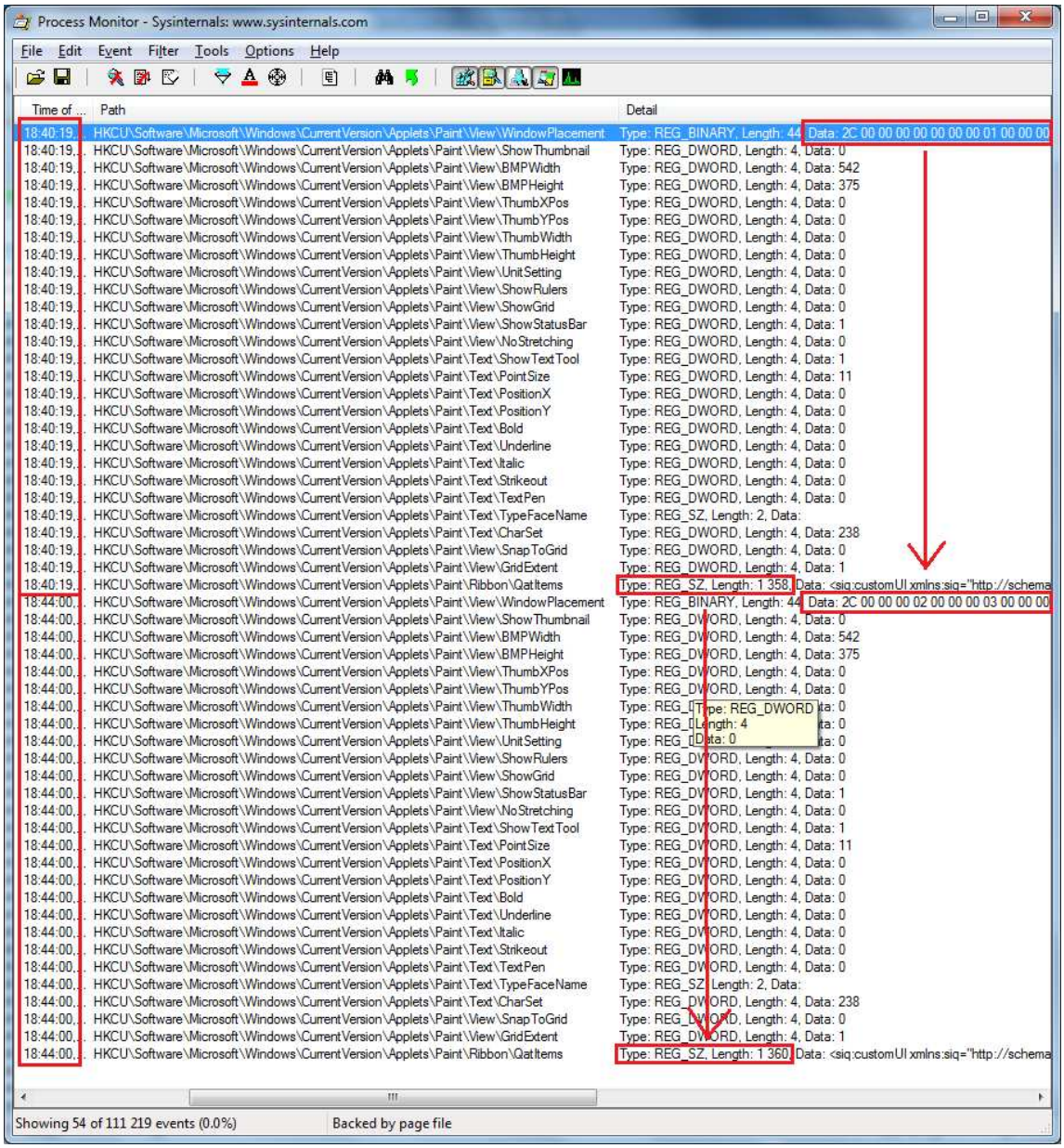


Obrázek č.16 - Zaznamenané události

g. Přizpůsobíme si zobrazení sloupců Process Monitoru tak, abychom viděli sloupce „Time“, „Path“, a „Detail“. Mezi jednotlivými spuštěními jsou patrné změny v hodnotách:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Ribbon\ QatItems
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\View\ WindowPlacement

h. Poznamenáme si důležité klíče a hodnoty a ukončíme program Process Monitor



Obrázek č.17 - Analýza změn po nastavení okna Malování

6.1.2.7 Zápis do registrů

a. Spustíme nástroj Regedit
b. Přesuneme se na klíč HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\View a exportujeme do souboru s názvem mspaint1.reg
c. Přesuneme se na klíč HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Ribbon a exportujeme do souboru s názvem mspaint2.reg
d. Ukončíme nástroj Regedit

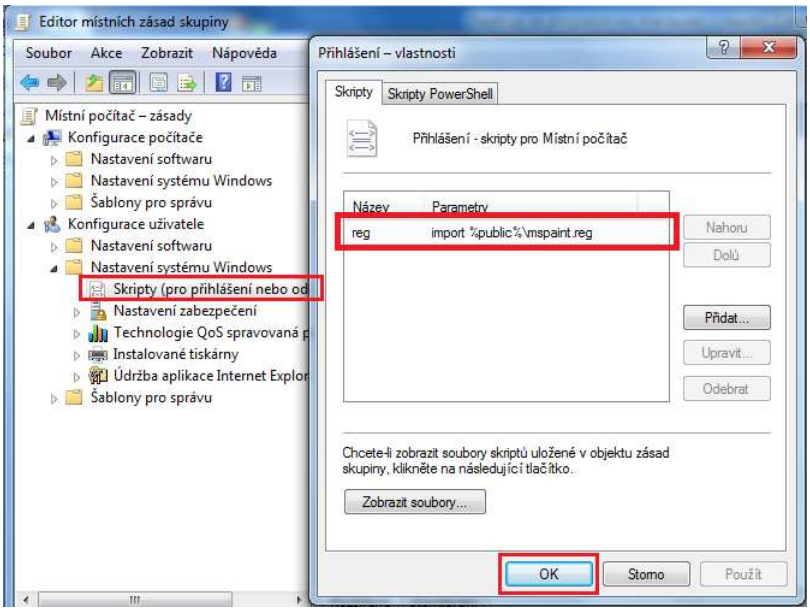
6.1.2.8 Sloučení registrů

Ze souborů mspaint1.reg a mspaint2.reg odstraníme nepotřebné hodnoty a sloučíme do jednoho souboru s názvem mspaint.reg.

Text obsahu sloučeného souboru mspaint.reg – příloha č.11

6.1.2.9 Zajištění aplikace souboru mspaint.reg pokaždé při přihlášení uživatele

a. Zkopírujte soubor mspaint.reg do adresáře %public% (např. C:\Users\Public).
b. Zajistíme spuštění příkazu "REG IMPORT%public%\mspaint.reg" vždy po přihlášení uživatele. Např. Pomocí editor místních zásad skupiny (gpedit.msc).



Obrázek č.18 - Import registru do Editoru místních zásad skupiny

6.1.3 Test funkčnosti celého řešení

a. Spustíme Malování, skryjeme pás karet, a co nejvíce zmenšíme okno.
b. Provedeme odhlášení přihlášeného uživatele
c. Po opětovném přihlášení se Malování spustí maximalizované se zobrazeným pásem karet, jak je požadováno.

7 Závěr

Práce byla zhotovena jako dokument, s jehož pomocí zvládneme parametrizaci systémového registru Windows 7 na potřebnou a předem zvolenou úroveň. Popisy a vysvětlení klíčů a registru jsem podal formou která je adekvátně podrobná účelu práce a s přílohami ho i překračuje, to však není ke škodě.

Doporučené a použité programy jsou legální a zadarmo. Nenastává tím tedy finanční přítěž pro školu či uživatele. Práci s nástroji jsem detailně popsal a obrazová dokumentace poslouží k lepšímu pochopení. Pro komplexnější doporučované aplikace jsou uvedeny příručky v přílohách. Přílohy na optickém médiu obsahují stažené programy, používání práce je tedy i tímto velice zjednodušeno.

Řešený demonstrativní příklad se sestavit podařilo úspěšně. Podmínka využití komplexních znalostí splněna byla. K jeho řešení musíme chápat strukturu registru, ovládat nástroj Regedit, upravovat REG soubory, pracovat s Editorem místních zásad skupiny a v neposlední řadě analyzovat probíhající procesy Process Monitorem.

Seznam zkratek byl vytvořen a je součástí práce.

8 Seznam použité a doporučené literatury

[1.] HONEYCUTT, Jerry. *Microsoft® Windows® Registry Guide, Second Edition*. [s.l.] : Microsoft, 2005. 608 s. ISBN 9780735622180.

[2.] HONEYCUTT, Jerry. *Registr MS Windows*. [s.l.] : COMPUTER PRESS , 2007. 590 s. ISBN 80-251-1265-9.

[3.] CAFOUREK, Bohdan. *Windows 7 - kompletní příručka*. [s.l.] : GRADA, 2010. 326 s. ISBN 8024703955.

[4.] NORDAHL-HAGEN, Petter. *Registry Editor Usermanual/docs* [online]. [s.l.] : [s.n.], 2010 [cit. 2011-04-03]. Dostupné z WWW: <http://pogostick.net/~pnh/ntpasswd/regedit.txt>.

[5.] *Moderní spravce* [online]. 2011 [cit. 2011-04-03]. Dostupné z WWW: <www.modernivyuka.cz/spravce>.

[6.] *Windows 7 forums* [online]. 2009 [cit. 2011-04-02]. Dostupné z WWW: <http://windows7forums.com>.

[7.] *Blogs.msdn.com* [online]. 18.2.2008 [cit. 2011-04-03]. Why do registry keys have a default value? - The Old New Thing - Site Home - MSDN Blogs. Dostupné z WWW: <http://blogs.msdn.com/b/oldnewthing/archive/2008/01/18/7145021.aspx>.

[8.] *Cloudapp.net* [online]. 2010 [cit. 2011-04-02]. Group Policy Search. Dostupné z WWW: <http://gps.cloudapp.net/>.

[9.] *FiveAndDime.net* [online]. 2011 [cit. 2011-04-02]. Windows 7 Notes, Registry, Hacks, Tips » Problem Solved:. Dostupné z WWW: <http://www.fiveanddime.net/windows7-notes/index.html>.

[10.] *Microsoft Technet* [online]. 2011 [cit. 2011-04-02]. Microsoft TechNet: Resources for IT Professionals:. Dostupné z WWW: <http://technet.microsoft.com>.

[11.] *Mintywhite.com* [online]. 2009 [cit. 2011-04-03]. Working with the Windows Registry (Windows 7, Vista, XP). Dostupné z WWW:

<http://mintywhite.com/windows-7/7security/working-with-the-windows-registry/>.

[12.] *Molikuv WEB* [online]. 2010 [cit. 2011-04-02]. Molikuv webik - Registry:. Dostupné z WWW: <http://www.molik.go.cz/tipy/registry.html>.

[13.] *Msdn.microsoft.com* [online]. 11. 2000 [cit. 2011-04-03]. Windows 2000 Registry: Latest Features and APIs Provide the Power to Customize and Extend Your Apps. Dostupné z WWW: <http://msdn.microsoft.com/cs-cz/magazine/bb985037%28en-us%29.aspx>.

[14.] *Msdn.microsoft.com* [online]. 4/10/2011 [cit. 2011-04-03]. Registry Hives (Windows). Dostupné z WWW: <http://msdn.microsoft.com/en-us/library/ms724877.aspx>.

[15.] *Navajo* [online]. 2010 [cit. 2011-04-02]. Registr oken. Dostupné z WWW: <http://registr-oken.navajo.cz/>.

[16.] *Pogostick.net* [online]. 27.6.2010 [cit. 2011-04-03]. Offline NT Password & Registry Editor. Dostupné z WWW: <http://pogostick.net/~pnh/ntpasswd/>.

[17.] *Support.microsoft.com* [online]. 3. 2011, 23. 4. 2011 [cit. 2011-04-03]. Using Registry Editor in Real Mode. Dostupné z WWW: <http://support.microsoft.com/kb/131352>.

[18.] *Support.microsoft.com* [online]. 4,10. 3.12.2007 [cit. 2011-04-03]. How to add, modify, or delete registry subkeys and values by using a registration entries (.reg) file. Dostupné z WWW: <http://support.microsoft.com/kb/310516/en-us>.

[19.] *Support.microsoft.com* [online]. 12.1. 12. 3. 2008 [cit. 2011-04-03]. Informace o registru systému Windows pro pokročilé uživatele. Dostupné z WWW: <http://support.microsoft.com/kb/256986>.

[20.] *Www.ibm.com* [online]. 5.6.2006 [cit. 2011-04-03]. The cranky user: Storing configuration data. Dostupné z WWW:

<http://www.ibm.com/developerworks/web/library/wa-cranky66a/index.html>.

[21.] *Www.microsoft.com* [online]. 2011 [cit. 2011-04-03]. Microsoft Windows Enterprise: Enhancing Group Policy. Dostupné z WWW: <http://www.microsoft.com/windows/enterprise/products/mdop/agpm.aspx>.

[22.] PETRI, Daniel . *Www.petri.co.il* [online]. 8.2.2009 [cit. 2011-04-03]. REG Command in Windows XP. Dostupné z WWW: <http://www.petri.co.il/reg_command_in_windows_xp.htm>.

[23.] *Www.winehq.org* [online]. 2011 [cit. 2011-04-03]. WineHQ - Using the Registry and Regedit. Dostupné z WWW: <http://www.winehq.org/docs/wineusr-guide/using-regedit>.

[24.] *Windows Guides* [online]. 2009 [cit. 2011-04-03]. Working with the Windows Registry (Windows 7, Vista, XP). Dostupné z WWW: <http://mintywhite.com/windows-7/7security/working-with-the-windows-registry>.

[25.] *Http://www.virtualbox.org* [online]. 2011 [cit. 2011-04-04]. VirtualBox. Dostupné z WWW: <http://www.virtualbox.org/wiki/Downloads>

9 Seznam zkratek a cizích slov

A

ACL - Seznam pro řízení přístupu (Access Control List): Nastavení oprávnění přístupu k objektu (soubor, klíč registru apd.) pro konkrétní uživatele.

B

BCD – Nastavení zaváděcích dat (Boot Configuration Data): Soubory a klíče s daty spouštěnými při startu systému.

BIOS – Základní vstupně-výstupní systém (Basic Input-Output Systém): Čip na základní desce PC s nahraným systémem obsluhující HW počítače.

Boot/ Bootování – Zavádění informací a dat při startu operačního systému.

C

CMD – (Command): Systémové prostředí pro práci v příkazovém řádku.

Cmdlety – specializované příkazy

D

DLL – Dynamicky linkovaná knihovna (Dynamic-link library): soubor knihovny systému

E

Editace – Úprava

G

GUI - Grafické uživatelské rozhraní (Graphical User Interface): Uživatelské rozhraní umožňující ovládat počítač pomocí grafických prvků.

H

HARDWARE – hmatatelné součásti PC

Hive, hives – Kořenové podregistry, klíče

HKEY_XXX – základní klíče registru

I

IEAK – Nastavení pro Internet Explorer (Internet Explorer Administration Kit):

Image – V kontextu práce myšleno jako bitová kopie optického disku.

INI Soubor – Soubor s nastavením

NTFS – Souborový systém (New Technology File System)

P

PE Médium – Samospustitelné médium (Preinstallation Environment): Používá se k testům, nebo k opravě systému

Plug-N-Play – „Zapoj a hraj“ : HW Zařízení umožňující připojení za chodu

R

Registr/Podregistr – Databáze nastavení systému

RNG –Generátor náhodných čísel (Random Number Generation)

S

Skript – Podpůrný program spouštěný systémem nebo aplikací

Systém – SW umožňující práci s PC, „To co vidíme“

Systém NT – typ operačního systému, používá registr, NT=New technology

T

Transakce – Skupina operací s registry, zahajuje se příkazem

U

Upgrade –Vylepšení

USB - Univerzální sériová sběrnice (Universal Serial Bus): slouží k připojení zařízení, např. Flash paměť, myš, scanner atd.

USMT – Nástroj pro migraci uživatele z PC na PC(User State Migration Tool)

V

Virtuální stroj – SW umožňující simulování počítače v „okně“

W

WAIK - (Windows Automated Installation Kit): sada nástrojů, umožňující zprovoznění automatizované instalace Windows 7

Windows XX – Operační systém