Řešení a implementace nástroje pro softwarový audit a dálkovou správu

Solutions and Implementation of Software Tool for Remote Management and Audit

Bc. Jiří ZUKAL

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ABSTRAKT

Tématem diplomové práce je komplexní řešení správy počítačů podnikové sítě, využívajících doménovou strukturu služby Active Directory na platformě Microsoft Windows. Zabývá se implementací nástrojů dálkové správy jednotlivých stanic, integrovaného systému podpory uživatelů, databází evidence licencí a provozovaného softwaru s možností provádění pravidelných či namátkových dálkových softwarových auditů. Nechybí ani analýzy technik pro skryté monitorování činnosti práce uživatelů na počítači, dále pak řešení datové bezpečnosti, dálkové hromadné instalace uživatelského software, možnosti řízení systémových prostředků vzdálených stanic či serverů, nasazování a uplatnění bezpečnostních politik a další užitečné postupy. Diplomová práce by měla čtenáři poskytnout jak teoretické informace, tak praktické možnosti řešení a realizace dálkové správy uživatelských stanic v infrastruktuře podnikové sítě.

Klíčová slova:

Active Directory, doména, Dozorce, informační portál, monitoring uživatelů, PCInfoMagicEYE, podpora uživatelů, softwarový audit, servisní kniha, VNC, vzdálená správa, zálohování dat.

ABSTRACT

The topic of the thesis is a computer network management comprehensive solution using the active directory domain configuration on Microsoft Windows platform. It deals with the implementation of the remote management tools on individual stations integrated system of user support licenses database record and running software operated with the possibility of execution or regular or random remote SW audits. Analysis techniques for monitoring the activities of the hidden work PC users are not omit as well as the data security solution, users SW remote public installations, possibilities of remote stations or servers SW systems managing, applying of security policies and many other useful techniques. The Diploma thesis should provide the reader with theoretical information and a practical possibilities of concrete solution as well as implementation of remote management of user workstation in the network business infrastructure.

Keywords:

Active Directory, Backups, Dozorce, Information Portal, Monitoring Users, PCInfoMagicEYE, Software Audit, Service Book, Remote Administration, Remote Installation, User Support, VNC.

Poděkování

Na tomto místě bych rád a ze srdce poděkoval svému konzultantovi, panu Miloslavu Jandovi z oddělení OAI Finančního ředitelství v Hradci Králové. Dále pak panu Ing. Vladimíru Dvořákovi z firmy FairNet s. r. o. za pomoc a poskytnuté informace týkající se aplikace PCInfoMagicEYE a panu Mgr. Janu Konečnému z firmy FairNet s. r. o. za informace z legislativní oblasti. Za korekturu překladů do anglického jazyka děkuji panu Ing. Janu Králíkovi. Za recenze, neobyčejnou trpělivost, lásku, podporu a pochopení vyjadřuji úctu a hlubokou poklonu paní MUDr. Janě Pimerové.

Zvláštní poděkování za vedení diplomové práce, odborné konzultace a velmi vstřícnou spolupráci patří paní doc. Ing. Zdence Prokopové, CSc.

Typografické konvence

V textu je použito několik typů písma pro odlišení různých skupin informací. Kromě základního textu jsem použil *kurzívu,* kterou odlišuji konvenční názvy produktů, technologií, hardwaru a softwaru. Dále pak *„kurzívou“* v uvozovkách označuji názvy dílčích součástí produktů a programových funkcí. Tučnou ***kurzívu*** užívám k označení názvů systémových služeb, příkazů, spustitelných či datových souborů nebo jejich přípon. Velkou *KURZÍVOU* jsou zpravidla značeny zkratky, které jsou vysvětleny ve slovníčku na konci diplomové práce. Pokud je někde použité písmo Verdana, jde o **syntaxi zápisu zdrojového kódu**.

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....10
I. TEORETICKÁ ČÁST....11
1 SÍŤOVÁ ARCHITEKTURA WINDOWS....12
1.1 Síťové komponenty Windows....12
1.2 Síťová rozhraní API....14
1.2.1 Nastavení síťových služeb Windows....14
1.2.2 Topologie a struktura sítě....18
1.2.3 Active Directory....19
2 TECHNICKÁ PODPORA UŽIVATELŮ....19
2.1 Strategie podpory uživatelů....19
2.2 Intranetový informační portál....20
2.2.1 Implementace informačního portálu....20
2.3 Servisní kniha versus HelpDesk....21
2.4 Prostředky vzdáleného připojení....24
2.4.1 Vzdálená plocha a vzdálená pomoc Windows....24
2.4.2 Povolení nebo zakázání vzdálené plochy....25
2.4.3 Software třetích stran pro dálkové ovládání počítačů....27
3 PROSTŘEDKY AUDITU A VZDÁLENÉ SPRÁVY....28
3.1 Softwarové aplikace pro audit počítačů....28
3.2 Architektura aplikace PCInfo MagicEYE....28
3.2.1 PCInfo server....29
3.2.2 PCInfo desktop....29
3.2.3 PCInfo klient a agent....30
3.2.4 Komunikace mezi komponentami PCInfo MagicEYE....31
3.3 Možnosti užití aplikace PCInfo MagicEYE....32
3.3.1 Automatická detekce Hardware a Software....32
3.3.2 Vyhodnocení softwarového auditu a jeho výstupy....32
3.3.3 Nástroje pro IT managery....33
3.3.4 Řídicí centrum sítě....33
3.3.5 Dálkové ovládání počítačů....34
3.3.6 Interní softwarový a hardwarový audit....35

3.4 Rozšíření aplikace PCInfo MagicEYE....35
3.4.1 MagicMONITOR....35
3.4.2 MagicDESK....36
4 NÁSTROJE PRO SLEDOVÁNÍ ČINNOSTI UŽIVATELŮ....37
4.1 Morální hlediska sledování práce zaměstnanců na počítačích....37
4.1.1 Etický pohled....38
4.2 Právní aspekty....38
4.2.1 Ochrana osobních práv zaměstnance....38
4.2.2 Monitorování elektronické pošty, ochrana soukromí a osobních údajů. .39
4.2.3 Porušování tajemství dopravovaných zpráv....40
4.2.4 Zásah do soukromí a porušení listovního tajemství....41
4.3 Volba vhodného monitorovacího systému....41
5 BEZPEČNOST UŽIVATELSKÝCH A PROVOZNÍCH DAT....42
5.1 Ochrana dat před jejich ztrátou a poškozením....42
5.1.1 Obecné požadavky na zálohovací software....43
5.1.2 Analýza vlastností zálohovacího softwaru....44
5.1.3 Výběr zálohovacího software....45
II. PRAKTICKÁ ČÁST....46
6 REALIZACE SOFTWAROVÉHO AUDITU....47
6.1 Audit aplikací PCInfo MagicEYE....47
6.1.1 Konfigurace softwarového auditu....47
6.1.2 Výsledky softwarového auditu....49
6.1.3 Hodnocení PCInfo MagicEYE....50
6.2 Audit aplikací WinAudit....50
7 MONITOROVÁNÍ UŽIVATELSKÝCH AKTIVIT....51
7.1 Monitorovací systém Dozorce....51
7.1.1 Instalace programu Dozorce....51
7.1.2 Nastavení a provoz programu Dozorce....53
7.1.3 Sumarizace nasbíraných dat v grafech a tabulkách....53
7.1.4 Hodnocení programu Dozorce....57
7.2 Monitorovací program ManicTime....57
7.2.1 Instalace a nastavení programu ManicTime....58
7.2.2 Provoz aplikace ManicTime....58
7.2.3 Hodnocení programu ManicTime....58

8 NÁSTROJE VZDÁLENÉ SPRÁVY 61
8.1 Speciální aplikace WinGrab.....61
8.2 Jednoduché řešení diagnostiky soketovou testovací funkcí 61
8.3 Problémy se spuštěním auditu PCInfo MagicEYE 63
8.4 Logon skript pro potřeby vzdálené správy.....63
8.4.1 Instalace programu z logon skriptu.....64
8.4.2 Instalace programu z Active Directory.....65
8.4.3 Importování klíčů systémového registru.....66
8.5 Plánovač úloh Windows.....67
8.6 Total Commander.....68
8.7 Nástroje PS Tools.....69
8.8 Skupina příkazů NET 71
9 ZÁLOHOVÁNÍ A ARCHIVACE DAT.....72
9.1 Symantec Backup Exec.....72
9.2 Freeware pro zálohování dat.....73
ZÁVĚR.....75
ZÁVĚR V ANGLIČTINĚ.....76
SEZNAM POUŽITÝCH ZKRATEK.....77
SEZNAM POUŽITÉ LITERATURY.....82
SEZNAM OBRÁZKŮ.....85
SEZNAM PŘÍLOH.....86

ÚVOD

Obecnou problematiku komplexní správy počítačových sítí v podnikových doménách nebo pracovních skupinách řeší každý administrátor na lokální nebo globální úrovni. Podstatou vzdálené správy je mít centrální dohled a kontrolu nad funkční infrastrukturou spravované autonomní datové sítě. Prvky takové sítě mohou být routery, modemy, switche, wi-fi rozhraní, servery, databáze, datové sklady, uživatelské pracovní stanice, systémy *EZS* a *EPS*, IP telefony, docházkové terminály, nebo jiná sdílená periferní zařízení, například tiskárny, scannery, kopírovací stroje a další. Prostorově rozlehlé datové sítě vyzývají k hledání různých způsobů zjednodušení práce a zajištění jejich spolehlivosti. Jde především o možnost vzdálené správy, řízení a kontroly koncových zařízení a prvků mezi nimi.

Dálková správa serverů či počítačů je naprosto komfortním řešením případných technických, aplikačních nebo systémových problémů, a to převážně z hlediska relativně okamžitého zásahu, bez ohledu na reálnou vzdálenost mezi spravovaným zařízením a technikem. Formu identifikace dnes řeší různé implementace podpůrných systémů *HelpDesk* a informačních portálů.

K dalším oblastem správy výpočetní techniky a vybavení počítačů patří hardwarový a softwarový audit, čili kontrola a evidence hmotného a nehmotného majetku. Pomocí takových auditů lze pak jednoduše dohlížet na dodržování stanovené koncepce povoleného užívaného softwaru a hardwaru. Definice přístupových práv k dílčím fyzickým a logickým objektům sítě vymezují bezpečnostní a personální politiky. Ty zpravidla určují manažeři firem a organizací. Jako jednu z součástí komplexní správy počítačových sítí nelze opomenout strategii datové bezpečnosti, spolehlivého zálohování a archivaci dat.

Kontroverzní problematikou současné doby se stává softwarový monitoring činnosti zaměstnanců na pracovních počítačích a následné hodnocení efektivního využívání pracovní doby.

Cílem diplomové práce je nalézt a implementovat softwarová řešení pro výše uvedené oblasti komplexní správy podnikové sítě. K realizaci jsem primárně volil komerční software, uvádím však také alternativy z volně dostupného freeware či *Open Source* a některá vlastní specifická řešení. Část diplomové práce obsahuje analýzu české legislativy platné pro rok 2010 o možnosti legálního užívání monitorovacího software určeného pro proces sledování činnosti zaměstnanců.

I. TEORETICKÁ ČÁST

1 SÍŤOVÁ ARCHITEKTURA WINDOWS

Úkolem síťového software je převzít I/O požadavek z aplikace na jednom počítači, poslat jej na vzdálené PC, na něm pak požadavek provést a výsledek předat zpět na původní počítač. Toto je velmi zjednodušená definice procesu síťové komunikace mezi počítači, během něhož se požadavek a odpověď na své cestě několikrát transformuje. Pro lepší názornost poslouží standard z roku 1983, tedy *Referenční model OSI.* Model *OSI* definuje sedm vrstev. V architektuře TCP/IP jsou zastoupeny pouze vrstvy čtyři. Vzájemné datové transformace provádějí na jednotlivých vrstvách modelu aplikační a komunikační protokoly, jak je znázorněno na obrázku Obrázek 1.

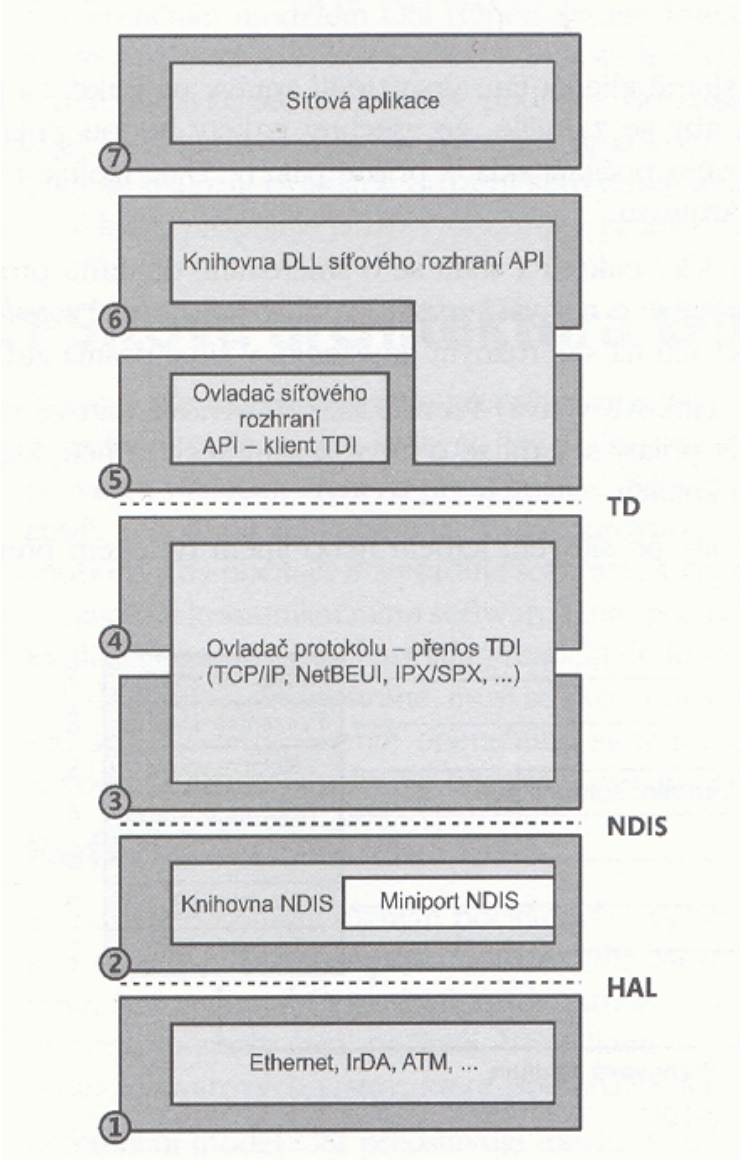
Referenční model OSI představuje idealizované schéma, které se přesně realizovalo jen na málo systémech, spíše slouží jako vizualizovaná hierarchie datových transformací z vyšší (aplikační) úrovně na nižší (bitovou) komunikační vrstvu. Účelem každé vrstvy modelu OSI je zajišťovat služby pro vyšší vrstvy a izolovat je od způsobu realizace služeb na nižších vrstvách [5].

<table>
<tr><th>OSI</th><th>TCP/IP</th><th colspan="8">Aplikace a protokoly</th></tr>
<tr><td>7. aplikační
6. presentační
5. relační</td><td>Aplikační vrstva</td><td>telnet</td><td>FTP</td><td>TFTP</td><td>SMTP</td><td>RIP</td><td>DNS</td><td colspan="2">Ostatní</td></tr>
<tr><td>4. transportní</td><td>Transportní vrstva</td><td colspan="4">TCP</td><td colspan="4">UDP</td></tr>
<tr><td rowspan="2">3. síťová</td><td rowspan="2">Síťová vrstva</td><td colspan="4" rowspan="2">IP</td><td colspan="2">ICMP</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>ARP</td><td>RARP</td></tr>
<tr><td>2. linková
1. fyzická</td><td>Vrstva síťového rozhraní</td><td colspan="3">token ring</td><td colspan="3">ethernet</td><td colspan="2">jiné typy protokolů</td></tr>
</table>

Obrázek 1: Referenční model OSI [23]

1.1 Síťové komponenty Windows

Na obrázku Obrázek 2 je vidět softwarové uspořádání síťové architektury Windows, které nekoresponduje s výše uvedeným, obecným modelem OSI. Například přenosy TDI velmi často překračují několik hranic. Skutečností je, že první čtyři vrstvy jsou nazývány "přenosem", kdežto horní tři vrstvy se nazývají "uživatelé přenosu".



Obrázek 2: Síťová architektura Windows [5]

- ***Síťové rozhraní API*** – poskytuje aplikační prostředky pro komunikaci mezi sítěmi nezávisle na protokolu. Používá se pro libovolné programovací rozhraní poskytované softwarem spojeným se sítěmi.
- ***Klienti rozhraní transportního ovladače TDI*** *(Transport Driver Interface)* – ovladače zařízení běžící v režimu jádra systému. Obvykle realizují tu část implementace síťového rozhraní *API*, která je určena pro režim jádra.

- ***Ovladače protokolu NDIS*** *(Network Driver Interface Specification)* – představují ovladače protokolu běžící v režimu jádra operačního systému. Přenosy TDI obecně usnadňují aplikační síťovou komunikaci tím, že transparentně provádějí operace se zprávami, jako např. jejich rozdělování a opětovné sestavování, seřazování, potvrzování a opakované vysílání.
- ***Knihovna NDIS (Ndis.sys)*** - zapouzdřuje ovladače adaptéru tím, že před nimi skrývá specifika prostředí jádra operačního systému Windows. Tato knihovna exportuje funkce používané přenosy TDI i podpůrné funkce určené ovladačům adaptérů.
- ***Ovladače miniportu NDIS*** – Ovladače miniportu NDIS komunikují se síťovými adaptéry prostřednictvím funkcí knihovny NDIS, které přecházejí do funkcí HAL (Hardwarové abstraktní vrstvy).

1.2 Síťová rozhraní API

Pro hlubší porozumění jednotlivým komponentám a vazbám v síťové architektuře Windows, doporučuji specializovanou literaturu [5]. Jejich popis je nad možný rámec této diplomové práce. Zde uvedu pouze výčet síťových služeb a protokolů rozhraní API Windows, jejichž nastavení a funkce jsou pro nás z pohledu dálkové správy zajímavé.

1.2.1 Nastavení síťových služeb Windows

- ***Brána firewall (ICF) / Sdílení připojení k internetu (ICS)*** – V chráněné doméně můžeme na jednotlivých stanicích službu zakázat. Ušetříme si tak mnoho času a starostí s pozdějšími „záhadnými“ problémy v komunikaci mezi síťovými prostředky.
- ***Centrum zabezpečení*** – Monitoruje nastavení zabezpečení systému (firewallu, antiviru apod.) a upozorňuje uživatele na jejich nedostatky. Ve spravované chráněné síti doporučuji na jednotlivých stanicích tuto službu deaktivovat. Generuje mnoho informačních „bublin“ v taskbaru, zvláště pak, pokud ponecháme deaktivovaný Firewall.
- ***Klient DHCP*** – Umožňuje automatickou konfiguraci síťového připojení, pokud je v síti spuštěný a nakonfigurovaný *DHCP* server. Jestliže používáme statické IP adresy na lokálních stanicích, doporučuji tuto službu přepnout do módu "Ručně".

- ***Klient DNS*** – Vyhledává a dočasně ukládá *DNS* záznamy (doménová jména a jim přiřazené IP adresy počítačů) pro budoucí použití. Pokud službu zakážeme, počítač se nebude dotazovat *DNS* serverů na překlad doménových jmen na IP adresy, což prakticky znemožní prohlížení webu při zadání adresy ve jmenném tvaru . Službu ponecháme v implicitním nastavení.
- ***Kurýrní služba*** – Služba pro zasílání krátkých zpráv prostřednictvím příkazu ***net send*** na *TCP* portech 135, 139, 445 a *UDP* portech 135 a 137. Zaslaná zpráva, například od administrátora serveru adresovaná vzdálené stanici dle jejího *DNS* názvu či IP adresy se objeví na cílovém počítači v malém modálním okně. Obsahuje text zprávy, název, IP adresu počítače či serveru, ze kterého byla odeslána. V chráněné doméně doporučuji nechat tuto službu na stanicích aktivní. Může se hodit pro hromadné odeslání důležitých informací na všechny spravované počítače volbou adresy broadcast.
- ***Oznamování systémových událostí*** – Sleduje systémové události, jako například přihlášení k systému, síťové události, nebo události týkající se napájení počítače. Ponecháme výchozí nastavení.
- ***Plánovač úloh*** – Umožňuje konfigurovat automatické spouštění úloh. Tato služba nachází širšího využití v unixových operačních systémech, kde je známá jako daemon ***cron***. Kreativní správce sítě dokáže tuto službu četně užívat i ve Windows. Službu ponecháme nastavenou na "Automaticky". Lze ji také dálkově konfigurovat například pro různé údržby systému.
- ***Podpora rozhraní NetBIOS nad protokolem TCP/IP*** – Podpora pro práci se síťovými jmény počítačů. I při vypnutí této služby by měly být jména počítačů dále dostupné přes překlad IP adresy. U počítačů připojených přímo do sítě Internet je vhodné službu zakázat. V případě spravované lokální sítě ji ponecháme aktivní spouštěnou automaticky. Nasazení aplikace *PCInfoMagicEYE* pro softwarový a hardwarový audit vyžaduje ponechat tuto službu spuštěnou.
- ***Kompatibilita pro rychlé přepínání uživatelů*** – Službu ponecháme v implicitním nastavení na automatické spouštění. Pro korektní funkci *Vzdálené plochy Windows* je ale důležitá.
- ***NetMeeting - Vzdálené sdílení plochy*** - Umožňuje pomocí aplikace ***NetMeeting*** vzdálený přístup k počítači. Aplikaci ***NetMeeting*** nepoužijeme, proto je pro naše účely vzdálené správy PC nevýznamná. Můžeme ji deaktivovat a zakázat její spouštění.

- ***Pracovní stanice*** - Vytváří a udržuje síťové připojení stanice jako klienta ke vzdáleným serverům, např. ke sdíleným složkám či tiskárnám. Tuto službu je nutné ponechat ve výchozím nastavení automatické aktivace.
- ***Server*** - Umožňuje lokálnímu počítači sdílet soubory, tiskárny a jiné systémové prostředky. Její deaktivaci u počítačů určených pro vzdálenou správu můžeme zcela jistě vyloučit.
- ***Prohledávání počítačů*** - Tato služba vytváří a udržuje seznam počítačů a dalších zdrojů v dostupných sítí. Službu ponecháme aktivní v módu „Automaticky“.
- ***Přihlašování k síti*** - Používá se pro přihlášení do domény. Ponecháme výchozí nastavení "Automaticky".
- ***Sekundární přihlašování*** - Umožňuje spouštění procesů s jiným pověřením. Pokud uživatelé pracují s omezenými právy, lze se přes kontextové menu pravého tlačítka myši, při kliknutí na požadovaný program v aktuálním sezení uživatele k programu přihlásit s oprávněním administrátora. Tato možnost je užitečná pro instalace programů přes vzdálenou plochu programu dálkového ovládání *VNC* v aplikaci *PCInfoMagicEYE*. Nastavíme na "Automaticky" a ponecháme ji aktivní.
- ***Síťová schránka*** - Umožňuje ukládání informací (vyjmout/vložit) a jejich sdílení s ostatními počítači. Občas se může hodit, zvláště při užívání vzdálené plochy ke správě serverů pro kopírování textů logů na lokální počítač. Služba je implicitně zakázána. Můžeme změnit její nastavení na "Automaticky" a spustit.
- ***Směrování a vzdálený přístup*** - Umožňuje počítačům připojit se přes modem či jiná zařízení k jiným sítím nebo vytvořit tunel *VPN*. Službu ponecháme deaktivovanou. Pro naše účely správy počítačů v rámci domény nebo lokální sítě nemá její aktivita význam.
- ***Správce automatického připojení pomocí vzdáleného přístupu*** - Při jakémkoli odkazu na název *DNS* či *NetBIOS* nebo adresu vzdáleného počítače vytvoří připojení ke vzdálené síti. Typ spouštění zvolíme na "Ručně". Může se hodit pro vytváření zástupců vzdálených složek nebo síťových disků.
- ***Správce vzdáleného přístupu*** - Služba automaticky mapuje a udržuje síťové adresy cílů připojení. To umožňuje přímé volání hostitele z aplikačního programu nebo z příkazové řádky. Cílovou adresou může být přímo název hostitele v Internetu, intranetu, IP adresa nebo název *NetBIOS* serveru. Ponecháme ji výchozí nastavení na "Ručně".

- ***Telnet*** – Služba dálkové správy pomocí příkazové řádky. Umožňuje přihlášení a připojení ke vzdálenému počítači s možností řízení jeho činnosti včetně spouštění programů. Velmi mocný nástroj, dnes však pro jeho malou bezpečnost nešifrované komunikace málo užívaný. V rámci dobře zabezpečené podnikové sítě či domény může být tento nástroj ale velmi užitečný. Výchozí nastavení služby je "Zakázáno". Budeme-li službu využívat, zvolíme typ spouštění na "Ručně".
- ***Terminálová služba*** - Umožňuje interaktivní připojení více uživatelů k počítači. Podporuje funkce vzdálené plochy, rychlého přepínání uživatelů, vzdálenou pomoc a terminálový server. Tato služba má pro práci dálkového ovládání počítačů zásadní význam a je důležité ponechat ji aktivní. Typ spouštění může být nastavený na "Ručně".
- ***Vzdálený registr*** - Umožňuje administrátorovi měnit nastavení systémového registru Windows vzdáleného počítače. Pomocí ***regedit*** se lze připojit a editovat registr vzdáleného systému, na kterém je tato služba spuštěna. Velmi užitečná pomůcka. Službu spustíme a typ spouštění nastavíme na "Automaticky".
- ***Windows Installer*** - Tato služba je nutná pro instalace softwaru pomocí balíčků s příponou ***msi***. Nastavení služby ponecháme ve výchozím nastavení "Automaticky" a spuštěnou. Programové instalační balíčky ***msi*** pro vzdálené hromadné instalace software jsou převážně užívány adresářovou službou *Active Directory.*
- ***Zasílání zpráv o chybách*** – Službu doporučuji deaktivovat. U méně zkušených uživatelů může při pádu některých aplikací vyvolávat značnou paniku vyskakující okno s nabízenou možnosti zasílání protokolu chyb na technickou podporu firmy Microsoft, .
- ***Služba WMI*** - Služba *WMI* (Windows Management Instrumentation) poskytuje integrovanou podporu datového modelu *CIM* (Common Information Model), který popisuje objekty existující v prostředí správy. Zprostředkovatelé služby *WMI* zajišťují komunikaci mezi službou *WMI* a součástmi operačního systému, aplikacemi a dalšími systémy. Poskytují informace o svých komponentách a mohou případně poskytovat metody pro práci s komponentami, vlastnosti, které lze nastavit, nebo události, které mohou uživatele upozornit na změny v komponentách. Pak je nanejvýš nutné ponechat tuto službu aktivní, typ spuštění na „Automaticky“ .
- ***Spouštěč procesů serveru DCOM*** - Služba *DCOM* (Distributed Component Object Model) je proprietární technologií společnosti Microsoft pro komunikaci mezi softwarovými komponentami distribuovaných na počítačích připojených k síti. Službu ponecháme ve výchozím nastavení na „Automaticky“ a aktivní.

Uvedl jsem zde jen některé, ale z pohledu správce domény důležité síťové služby operačního systému Windows, u kterých je třeba provést kontrolu nastavení a činnosti. Toto je doporučená, nikoliv závazná konfigurace, se kterou mám praktické zkušenosti. Je tak zajištěn spolehlivý přístup ke všem počítačům a informacím o stanicích ve spravované doméně. Umožnuje dynamicky a flexibilně vykonávat centralizovanou správu všech počítačů a serverů v námi udržované, ale také řádně zabezpečené podnikové síti.

1.2.2 Topologie a struktura sítě

Veškeré implementace softwaru pro potřeby této diplomové práce jsou prováděné na počítačích a serverech v podnikové síti s doménou adresářové služby *Active Directory*. Topologie doménového lesa je stromově hierarchická, čili obsahuje podřízené doménové stromy s vlastními primárními a sekundárními doménovými řadiči *Active Directory*. Dílčím doménám je nadřazen hlavní doménový server s globálním katalogem adresářové služby *Active Directory*, jehož databáze se jednou denně v noci replikuje na podřízené doménové řadiče [2].

Softwarové aplikace uvedené v této diplomové práci je samozřejmě možné implementovat i na jednoduché struktury sítí Microsoft Windows typu *Pracovní skupiny*. Nakonec v malých firmách, školách nebo jiných separátních institucích nejsou pokročilé doménové struktury nutné a vůbec potřebné. V obou případech je ale žádoucí, aby byly na síti přítomny výkonné servery (dva a více) s nepřetržitým provozem, které by měly mít tyto specifické role:

- ***WWW server*** (Portál místního intranetu, webové služby Internetu, *SQL* server, *PHP.*)
- ***PCInfo server*** (*SQL* server, *PCInfoMagicEYE* server)
- ***Backup server*** (Diskové pole, zálohování dat, archivace na pásky.)
- ***Print server*** (Síťové sdílené tiskárny, scannery, kopírovací stroje.)
- ***Proxy server*** (Internetová brána, Firewall, antivirová ochrana, *NAT, PAT.*)
- ***Poštovní server*** (např. Microsoft Exchange, antispamová ochrana..)
- ***File server*** (Úložiště datových souborů uživatelů, souborové databáze)
- ***Informační systém*** (Účetnictví, evidence zásob a majetku, objednávkový systém, systém pro řízení a správu organizace, personalistika atd.)

1.2.3 Active Directory

Návrhy organizovaných doménových struktur na síťové platformě *Microsoft Windows* služby *Active Directory* se zabývá speciální literatura [2]. Zde jen uvedu, že pomocí adresářové služby *Active Directory* lze jak na globální úrovni, tak na úrovni jednotlivých dílčích domén, realizovat bez obtíží mnoho úkonů týkajících se centralizované správy a řízení obsažených objektů (počítačů, serverů, tiskáren, uživatelských účtů atd.). Adresářová služba *Active Directory* a její tématika by zadala minimálně na další dvě diplomové práce.

Za zmínku však stojí, že umožňuje administrátorům centrálně vytvářet a spravovat skupiny objektů členěných do navržených organizačních skupin (role skupin jsou definovány většinou manažery organizací), na které můžeme aplikovat rozdílné bezpečnostní politiky a přístupová oprávnění k jiným fyzickým, logickým či datovým objektům.

Adresářová služba *Active Directory* umožňuje správcům velmi pohodlně provádět hromadné vzdálené instalace softwaru ze speciálně formátovaných balíčku ***msi*** služby ***Windows Installer***.

2 TECHNICKÁ PODPORA UŽIVATELŮ

2.1 Strategie podpory uživatelů

Volba vhodné filozofie a strategie podpory uživatelů je „alfou a omegou“ každodenní práce správců IT. Uživatele výpočetní techniky je třeba vést k pochopení zvyklostí a potřeb podniku, motivovat k učení, vstřebávání nových informací a k produktivní spolupráci. V první řadě je nutné vymezit hranice uživatelových možností a pravomocí pro řešení IT problematiky ve virtuálním prostotu a to nejlépe definicí přístupových práv. Ty pak určují, kde je třeba dbát na uživatelovi znalosti, pečovat o jejich zdokonalování, provádět osvětu a rozvíjet schopnosti dílčí asistence se správcem domény při řešení specifických problémů týkajících se např. vzdálených instalací softwaru. Vymezit jednoznačně tyto hranice není jednoduché. Efektivní strategií pro vzájemnou kooperaci se jeví flexibilní a permanentní zajištění informovanosti uživatelů. Prostředkem může být vhodně navržený webový intranetový informační portál. Ten je pak implicitně nastavený jako „domovská stránka“ webového prohlížeče.

2.2 Intranetový informační portál

Podnikový webový portál by měl být prvním zdrojem informací pro každého uživatele, který se přihlásí do domény. Měl by se zobrazovat implicitně po spuštění výchozího webového prohlížeče. V našem případě volím výchozím prohlížečem *Internet Explorer.* Důležité aktuální informace týkající se podniku tak mohou mít uživatelé ihned a přehledně k dipozici. Aby se vždy po startu PC a spuštění webového prohlížeče zobrazovala domovská stránka s informačním portálem, je dobré zajistit její trvalou předvolbu pro případ, že by si ji uživatel záměrně či omylem změnil. Máme několik možností:

Jednou z nich je definice vlastního pravidla místních zásad v modulu *„Group Policy Object Editor“* služby *Active Directory* na serveru doménového řadiče. Nastavení politiky provedeme na kontejneru s uživateli celého podniku. V nastavení místních zásad pak hledáme posloupnost těchto položek: *„Konfigurace uživatele“, Šablony pro správu“, „Windows Components“, „Aplikace Internet Explorer“*. Pro podrobnější informace k nastavení politik služby *Active Directory* doporučuji speciální literaturu [2].

Také můžeme využít dávkového souboru logon skriptu, který při každém startu uživatelské stanice a přihlášení do domény importuje klíč systémového registru, který zaktualizuje nastavení domovské stránky prohlížeče *Internet Explorer.*

Definování vlastních šablon místních zásad zabezpečení na úrovni služby *Active Directory* mi přijde jako mnohem elegantnější řešení, než příkazy prováděné z dávkového souboru logon skriptu, samozřejmě za podmínky, že službu *Active Directory* a doménové struktury užíváme.

2.2.1 Implementace informačního portálu

Pro realizaci portálu se mi jako nejvhodnější řešení zdála možnost využití licence *GNU/GPL* a engine redakčně-informačního systému *PHPRS 2.6.5* pro vytvoření vlastního podnikového informačního webového portálu. Pro služby web serveru jsem zvolil doporučený *VertrigoServ 2.21.* Softwarový balíček obsahuje tyto součásti:

- ***HTTP Apache 2.0.63***
- ***PHP 5.2.6***
- ***MySQL 5.0.51b***
- ***SQLite 3.5.9***
- ***PhpMyAdmin***
- ***SQLite Manager 1.2.0***
- ***Zend Optimizer 3.3.3***

Využil jsem moduly *HTTP Apache, PHP 5.2.6, MySQL 5.0.51b* a konfigurační prostředí *PhpMyAdmin*. Vzhled enginu *PHPRS 2.6.5* a většinu *PHP* kódu bylo třeba optimalizovat a patřičně upravit. Potřebné a užitečné pluginy vytvořit a doinstalovat. Konečnou podobu informačního portálu postaveného na enginu redakčně-informačního systému *PHPRS 2.6.5* zobrazuje Obrázek 3.

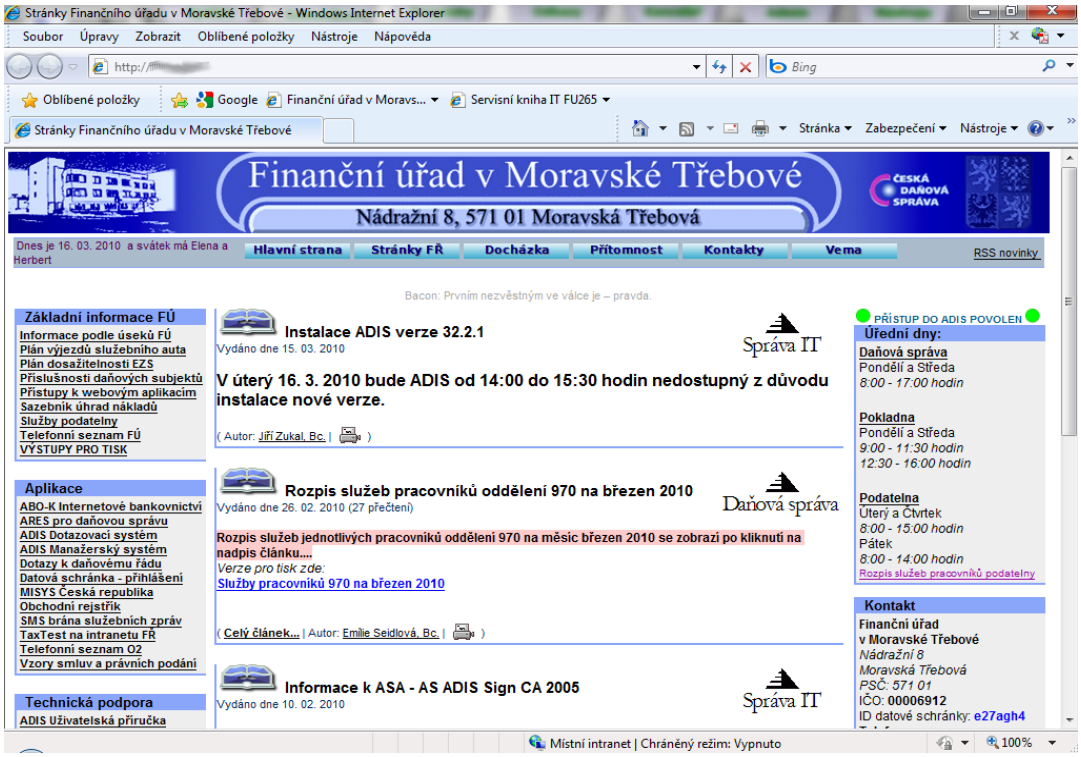
2.3 Servisní kniha versus HelpDesk

Interaktivní systémy *HelpDesk* jsou pro uživatele i pro samotné řešitele velmi vhodným komunikačním nástrojem. Umožňují převážně pomocí webového rozhraní uživatelům v klidu a přesně popsat závadu či daný problém, se kterým si neví rady a potřebují kvalifikovanou pomoc. Řešitelům a technikům pak tyto systémy umožňují řádně evidovat, vhodně řídit, efektivně organizovat a prakticky likvidovat zadané požadavky jednotlivých uživatelů. Některé robustní systémy *HelpDesk* komerčních a servisních firem obsahují také speciální moduly pro oceňování zakázek, fakturace a skladovou evidenci náhradních dílů.

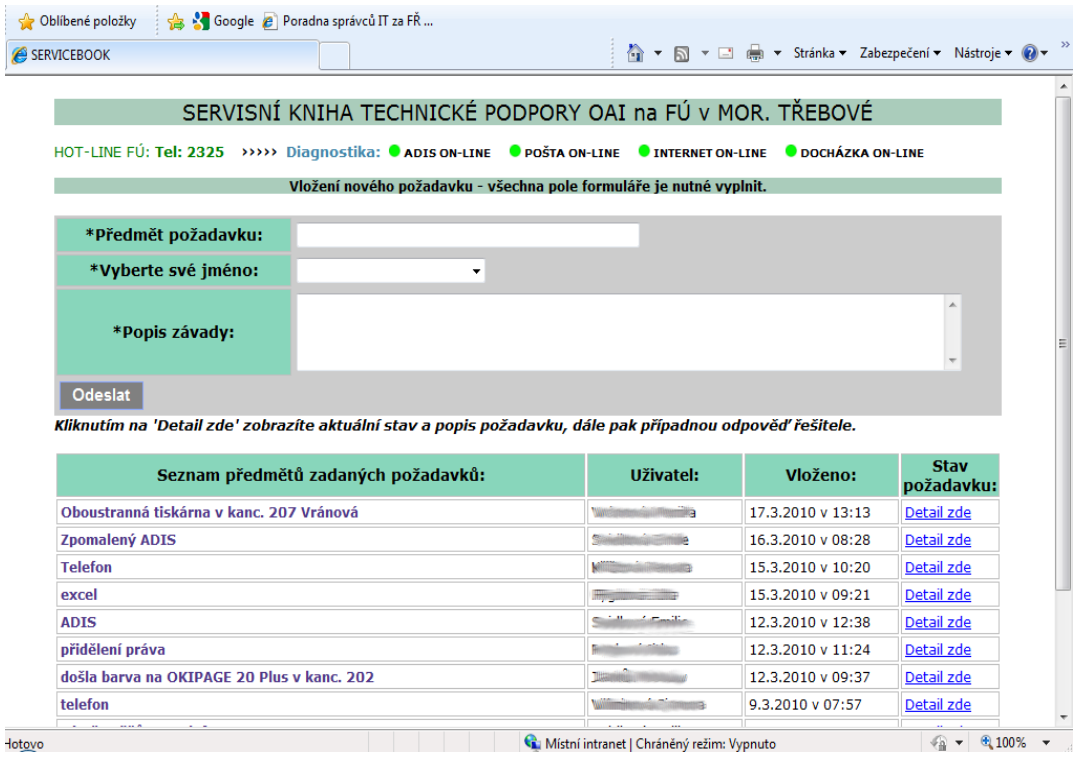
Jedno ze zadání diplomové práce je návrh a implementace vlastní aplikace pro podporu uživatelů. Na základě pečlivého průzkumu a analýzy požadavků uživatelů včetně vedoucích úseků a ředitele jsem procesním modelováním vytvořil návrh aplikace, kterou jsem pojmenoval *ServiceBook.* Z důvodu úspory místa v hlavní části diplomové práce jsem popis projektu aplikace *ServiceBook* (požadavky, diagram případů užití a diagram aktivit) umístil do přílohy Příloha I. Výsledkem je jednoduchá, intuitivní, transparentní, sdílená webová aplikace vytvořená v jazyku *PHP.* Není potřeba žádné registrace, žádného zdlouhavého vyplňování formulářů a studování manuálů. Samotný návrh aplikace musel vyhovět požadavkům uživatelů, že provedení bude maximálně jednoduché a neodradí uživatele komplikovaností či zadáváním nadbytečných údajů. Vložení požadavku musí být jednoduché a rychlé. Stejně tak i prohlížení dříve zadaných požadavků a výsledků řešení musí být snadné, transparentní, dostupné a přehledné. Na základě těchto žádostí jsem aplikaci navrhl jako analogii papírové „knihy oprav“ pro vkládání a evidenci servisních případů s popisem problému a jeho řešení. Podobné knihy oprav se v „dřevních“ dobách vedly v nevirtuální formě ve speciálně linkovaných sešitech a svému účelu dobře posloužily. Řešení vychází z filozofie „V jednoduchosti je síla“ nebo „Někdy méně znamená více“. Aplikace této servisní knihy zkrátka pokrývá místní potřeby uživatelů pro zadávání jejich požadavků pro správu IT.

Vzhledem k funkční jednoduchosti tohoto řešení jsem upustil od užití databázového stroje *MySQL*. Nižší složitost aplikace tak i výrazně snižuje pravděpodobnost její závady a možnou nedostupnost. Všechny zápisy v servisní knize se ukládají v textové podobě do indexových a datových souborů.

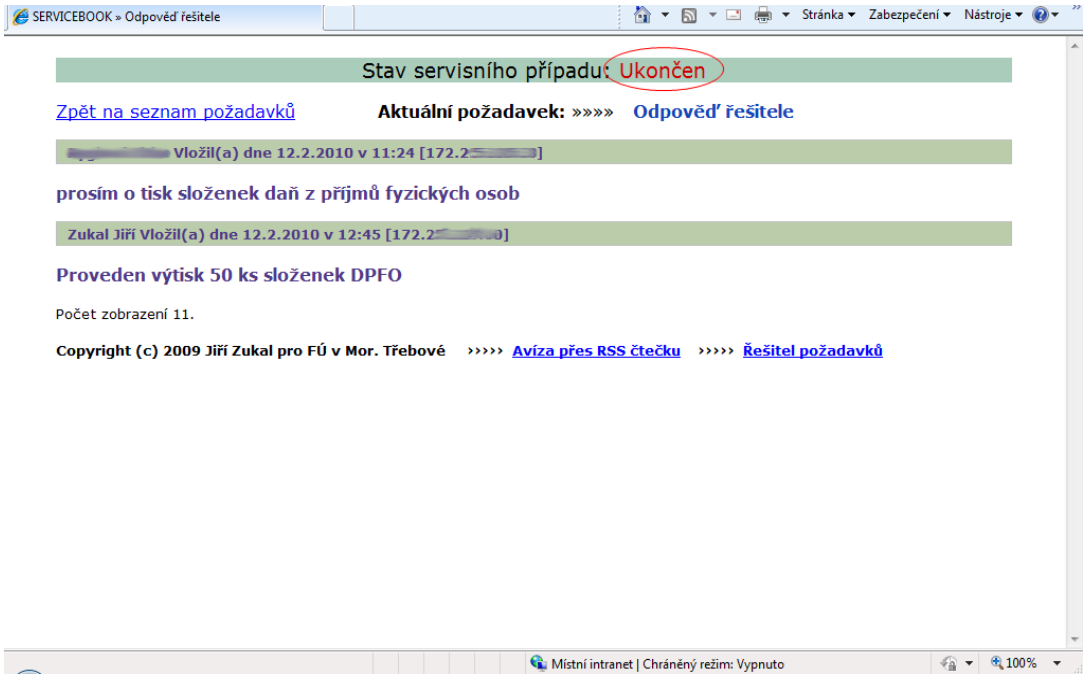
Celá aplikace je umístěná v jedné složce nazvané s***ervicebook***, umístěné v kořenovém adresáři *WWW* serveru. Bez nutnosti užití systému pro řízení báze dat je tak i jednoduše přenositelná. Má vlastní odkaz v podobě ikony zástupce umístěné na pracovní ploše Windows každého uživatele. Nadstavbou servisní knihy je informativní diagnostický panel viz Obrázek 4 některých provozovaných služeb. Signalizační barva návěští stavu testovaných služeb na tomto panelu uživatele informuje – viz Kapitola 8.2 o lokalitě problému (údržba informačního systému, výpadek proxy serveru, nefunkční elektronická pošta – *Microsoft Exchange,* nefunkční docházková aplikace provozovaná na vzdáleném serveru atd.). Panel také nabízí aktuální informaci na právě dostupný servisní „*Hot-line"* telefon. Aby se informace o zápisu do servisní knihy dostala včas k řešiteli, a aby měli vedoucí úseků stálý přehled nad danou situací, využil jsem možnosti odběrového kanálu *RSS*. Důvodem tohoto řešení je i to, že převážná většina uživatelů používá *RSS* čtečku *Feed Reader* pro odběr novinek portálu české daňové správy. Pro informaci o zápisu nové servisní události, která bude na vyžádání transparentní všem uživatelům včetně vedoucích úseků a ředitele, jsem *RSS* integroval do aplikace S*erviceBook*. K dispozici tak jsou všem uživatelům odkazy na zadané požadavky a případné odpovědi řešitele. Kliknutím na odkaz v došlém avízu libovolné čtečky *RSS* se uživateli otevře okno s detailem servisní událostí a aktuálním stavem řešení. Stejně tak bude vygenerováno nové avízo v případě změny stavu servisní události nebo při vložené odpovědi řešitele jak zobrazuje Obrázek 5**.** Použití avíz pomocí kanálu *RSS* nahrazuje odesílání informačních emailů, které užívá převážná většina *HelpDesk* systémů. *RSS* řešení poskytuje relativně okamžitou informaci všem on-line pracovníkům o tom, že jeden z nich již zadal servisní událost (požadavek k řešení) některého globálního problému. Do určité míry se tak zabrání duplicitnímu zadávání servisních případů ukazujících na stejný problém. Stejně tak bude dostupná odpověď řešitele na daný globální problém v jeden okamžik všem on-line uživatelům. Systém *RSS* nepotřebuje poštovní server, což je výhoda. *RSS* čtečka s oznamovacími „bublinami" o novinkách je rezidentně spouštěná na počítačích všech pracovníků ihned po startu Windows a aktualizaci avíz *RSS* nastavíme na pětiminutový interval.



Obrázek 3: Implementace podnikového informačního portálu



Obrázek 4: Servisní kniha pro podporu uživatelů



Obrázek 5: Informace o postupu a stavu řešeného požadavku

2.4 Prostředky vzdáleného připojení

Pro pokročilou správu stanic a serverů připojených do sítě je neocenitelnou pomůckou ***Terminálová služba Windows*** či jiné prostředky softwaru třetích stran určené pro vzdálené připojení. Terminálová služba je typem připojení *klient-server.* Přenáší klientovi uživatelské rozhraní programů běžících na serveru. Operace provedené klientem prostřednictvím klávesnice a myši jsou vraceny k provádění vzdálenému serveru. Sledování této činnosti zprostředkuje okno konzole terminálu na místním počítači, které zobrazuje prostředí vzdáleného systému. Obecně lze říci, že každý klient má po přihlášení k dispozici pouze vlastní relaci, která je transparentně spravována operačním systémem vzdálené stanice či serveru, a to nezávisle na jiných klientských relacích.

2.4.1 Vzdálená plocha a vzdálená pomoc Windows

Vzdálená plocha a ***Vzdálená pomoc*** jsou ve Windows dvě rozdílné služby, obě však mají společné terminálové připojení typu *klient-server.* ***Vzdálená plocha*** je funkce určená pro terminálové připojení uživatele jednoho počítače k jinému počítači na lokální nebo *VPN* síti. Přístupová práva pro vzdálenou plochu pak určuje členství ve skupině *„Remote Desktop Users“*. Slouží pro dálkovou správu a údržbu systému nebo instalaci software.

Vzdálená pomoc umožňuje dálkové připojení asistenta technické podpory Microsoft přes veřejný internet. Funkce musí být povolena ve vlastnostech systému a ve správě uživatelských účtů počítače je třeba mít povolený účet asistenta technické podpory. ***Vzdálená plocha*** Windows má jednu nespornou výhodu, na rozdíl od většiny software třetích stran. Je integrovanou složkou operačního systému Windows, a proto může správce systému svým vzdáleným přihlášením vykonávat všechny činnosti a funkce, jakoby seděl přímo u spravované stanice. Může vzdáleně odhlásit aktivní sezení uživatele s omezeným oprávněním a přihlásit se k účtu s vyšším oprávněním lokálního nebo doménového administrátora. Lze tak pohodlně vykonávat všechny rutiny správy a údržby uživatelských stanic či serverů. Za velký nedostatek „desktopových" edicí operačních systémů Windows považuji podporu pouze jednouživatelského režimu. Ten nedovoluje souběžné přihlášení více uživatelů k jedné stanici s jedním operačním systémem Windows. Jen pro zajímavost, linuxové distribuce pro desktopy multiuživatelský režim standardně podporují. Firma Microsoft multiuživatelský režim podporuje pouze u server edicí *Windows*, kde funkce ***Terminálové služby*** mohou souběžně užívat dva uživatelé. Za licenční příplatek lze multiuživatelský režim rozšířit na vyšší počet souběžných přihlášení. Klienta vzdálené plochy lze spustit z programové nabídky Windows nebo příkazem ***mstsc*** z příkazové řádky.

2.4.2 Povolení nebo zakázání vzdálené plochy

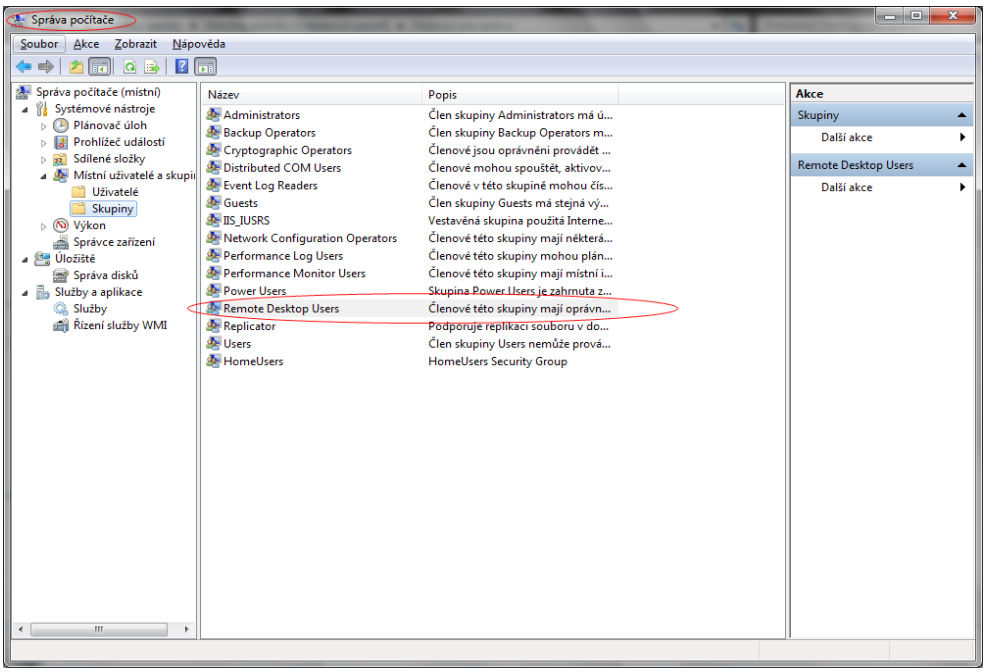
Ať už se rozhodneme, že funkci ***Vzdálená plocha*** Windows budeme či nebudeme používat, nastavení povolení nebo zákazu pro všechny stanice v doméně provedeme postupem pomocí zásad skupiny v modulu „*Group Policy Object Editor"* služby *Active Directory* na serveru řadiče domény. Vytvoříme si tedy nové pravidlo pro cílovou skupinu počítačů. Podrobnější informace o vytváření pravidel zásad skupiny služby *Active Directory* nalezne zvídavější čtenář ve speciální literatuře [2]. Zde uvedu pouze konkrétní definici tohoto pravidla:

Vytvoříme si nové pravidlo pro zvolenou organizační jednotku, skupinu počítačů nebo celý podnik a nazveme ho třeba *„Vzdalena_plocha_Windows"*. Ve složce *„Konfigurace počítače", „Šablony pro správu", „Součásti systému Windows", „Terminálová služba",* klikneme na položku *„Povolit uživatelům vzdálené připojení pomocí Terminálové služby"*. Zde nastavíme volbu *„Povolit"* a potvrdíme. Pokud povolíme službu ***Vzdálená plocha*** na stanicích v doméně, je třeba také rozhodnout, kteří doménoví uživatelé a skupiny se budou moci vzdáleně přihlásit.

Ty je nutné definovat na každé stanici zvlášť. Zvolené uživatele, v našem případě „*Domain Admins*“ poté ručně přidáme do skupiny „*Remote Desktop Users*“ na jednotlivých stanicích, samozřejmě také vzdáleně. V *Active Directory* to lze provést kliknutím pravým tlačítkem myši na vybrané stanice a v kontextovém menu vybrat volbu *„Spravovat“*. Zpřístupní se okno správy vzdálené stanice, jak zobrazuje Obrázek 6. Pak už můžeme jednoduše vkládat doménové uživatele do jednotlivých lokálních skupin vzdáleného správce na určených počítačích.

Důležitou poznámkou je, že všechny experimenty a změny v nastavení, které kdy budeme provádět v *Active Directory* pro uplatnění pravidla v rámci celé domény, podniku nebo určité skupiny je třeba nejprve náležitě otestovat. Pro tento účel si v *Active Directory* vytvoříme kontejner *„Testovací skupina“*, do kterého vložíme námi určené zkušební PC. Všechny nově definované politiky nastavení zásad skupiny pak řádně otestujeme pouze s uplatněním na zkušební počítač v testovací skupině. Teprve po řádném otestování můžeme provést přenos nové politiky do ostrého provozu na určenou skupinu počítačů a uživatelů.

Nastavení politik v *Active Directory* na serveru doménového řadiče vyžaduje práva doménového administrátora. Jakmile máme nastavené a přenesené politiky místních zásad na určenou skupinu počítačů a uživatelů v *Active Directory*, bude mít toto nastavení vždy vyšší prioritu, než jakékoliv nastavení stejné politiky místních zásad provedené lokálně na stanicích v této skupině. To samozřejmě platí, pokud se uživatel přihlásí ke svému doménovému účtu v *Active Directory*.



Obrázek 6: Správa počítače z Active Directory

2.4.3 Software třetích stran pro dálkové ovládání počítačů

Snad nejznámějším produktem mezi nástroji třetích stran pro vzdálenou správu počítačů je program *VNC* (Virtual Network Computing), a to v různých modifikacích. *VNC* pracuje jako distribuovaná aplikace typu *klient-server*, kde server vytváří grafickou plochu v operační paměti hostitelského počítače a komunikuje přes síť s klientem, který plochu zobrazuje správci na jiném počítači. Pro komunikaci se používá protokol *RFB (Remote Framebuffer)* [8], jehož cílem je minimalizovat objem přenášených dat mezi klientem a serverem a umožnit snadnou komunikaci přes pomalejší datové linky (např. přenos mezi modemy na analogových linkách). Různé modifikace a nadstavby *VNC* jako třeba *Tight VNC, Ultra VNC, VNC Thumbnail Viewer* a další jsou volně ke stažení na Internetu. Dalšími zajímavými aplikacemi pro dálkové připojení a ovládání počítače jsou *Hidden Administrator* nebo *LogMeIn*. Zatímco *Hidden Administrator* je aplikačním rozšířením *VNC, LogMeIn* je nástroj typu „midleware“, který pro správu vzdáleného počítače využívá běžný webový prohlížeč na straně klienta, dále pak zprostředkovatele spojení a zobrazení na veřejném Internetu mezi klientem a vzdáleným počítačem.

Zajímavé možnosti poskytuje vzdálená správa pomocí příkazové řádky. Dříve byl velmi oblíbeným nástrojem vzdálené správy ***Telnet***. Praktická je sada nástrojů *PS Tools*, *Resource Kit Tools Microsoft* nebo v systému Windows rezidentní skupina příkazů ***net***. Příkazová řádka sice není příliš v oblibě, ale implicitní systémové či explicitně dodané konzolové programy z ní činí velmi mocný nástroj [7]. Efektivní a korektní užívání příkazové řádky a příkazového interpretu závisí také na konkrétní užívané edici operačního systému Windows. Dále pak může mít vliv na užívání některých příkazů verze instalovaného ***ServicePack*** nebo bezpečnostní aktualizace systému. Konzolové nástroje pro správu systému vyžadují ke svému spuštění vyšší oprávnění, čili program příkazové řádky ***cmd.exe*** musí být spuštěný pod účtem správce systému. Bezpečnostní aktualizace Windows mohou mít vliv na korektní užívání softwaru třetích stran z řady nástrojů pro vzdálenou správu. U některých takových nástrojů se mohou po aplikaci bezpečnostních aktualizacích operačního systému Windows objevit znaky nestability či úplné disfunkce. V horších případech se stává, že některé programy třetích stran určené pro vzdálená připojení jsou vyhodnocovány antivirovým software jako škodlivý kód (tzv. Back Doors) a nekompromisně smazány.

3 PROSTŘEDKY AUDITU A VZDÁLENÉ SPRÁVY

3.1 Softwarové aplikace pro audit počítačů

Zjednodušeně řečeno jde o specifické softwarové nástroje, které slouží pro automatizovanou správu, kontrolu a evidenci nakoupeného (či jinak získaného), užívaného HW a SW vybavení počítačů. Jaké jsou hlavní přínosy takových aplikací? Uvedu zde ty zásadní:

- Poskytuje informace o efektivním využívání IT prostředků.
- Generuje podklady pro plánování a kvalifikovaný rozpočet dalšího rozvoje IT.
- Automaticky detekuje softwarové a hardwarové konfigurace počítačů.
- Získává přehled nad infrastrukturou počítačové sítě.
- Ulehčuje administrativu - generuje předávací protokoly, specifikační listy.
- Integruje nástroje pro správu pracovních stanic – dálkové ovládání počítačů.
- Spravuje agendu o zakoupených licencí SW.
- Umožní pohodlnou práci s daty – filtrování, SQL vyhledávání, exporty do různých formátů.
- Poskytuje možnosti komplexní správy majetku IT.
- Zachycuje historii změn – sledování změn v HW a SW konfiguraci mezi jednotlivými uskutečněnými audity.

Na Internetu je k dispozici celá řada produktů, které řeší tuto problematiku. Z českých komerčních programů mohu jmenovat například *AuditPro* [17], *PCInfo* [14] nebo *Alwao* [24]. Podrobnějším studiem jednotlivých produktů zjistíme, který bude našim potřebám vyhovovat nejvíce. Samozřejmě je také rozhodujícím kritériem cena takového software na požadovaný počet licencí. Lze volit také alternativy z volně dostupného software pod licencí *GNU/GPL* nebo freeware. Velmi povedený freeware, bez nutnosti instalace je program *WinAudit* [20]. Více informací o tomto produktu je uvedeno v praktické části diplomové práce a v příloze Příloha III.

3.2 Architektura aplikace PCInfo MagicEYE

Z výše uvedených variant jsem pro řešení zadaného tématu diplomové práce vybral softwarový balík distribuovaných nástrojů typu klient-server *PCInfo MagicEYE* od firmy *FairNet spol. s r. o.* Jde o soubor velmi povedených nástrojů pro komplexní správu podnikových sítí, který vyhoví vysokým nárokům manažerů firem i správcům IT.

Základní balík *PCInfo MagicEYE* disponuje nástroji pro správu, audity, evidenci a vyhodnocení počítačového vybavení s možností rozšíření o nadstavbové komponenty *MagicDESK* a *MagicMONITOR,* které lze zakoupit separátně. Nyní se podívejme na jednotlivé komponenty aplikace *PCInfo MagicEYE.*

3.2.1 PCInfo server

Instaluje se zpravidla na jeden z dostupných serverů v síti nebo doméně. Tato komponenta běží nad databází SQL a poskytuje datové služby pro své klienty. *PCInfo server* je také struktura sdílených adresářů s aktualizovanými instalačními balíčky aplikací *PCInfo desktop* a *PCInfo klient*. *Pcinfo MagicEYE* je tedy aplikací, která využívá pro svoji činnost služeb *MS SQL* serveru. V instalačním balíčku *Pcinfo MagicEYE* je obsažen *SQL Server Express Edition* (volně dostupná forma *MS SQL serveru 2005*, limit velikosti jedné databáze je 4 GB) nebo také *MSDE* (volně dostupná forma *MS SQL serveru 2000*). *MSDE* je omezeno objemem dat do 2 GB v jedné databázi. Takový objem dat pro zajímavost představuje cca 800 otestovaných počítačů uložených v databázi.

Do databáze komponenty *PCInfo server* se ukládají veškeré informace o aplikačním a uživatelském nastavení *PCInfo MagicEYE*, vedeném a auditovaném softwaru, o hardwaru spravovaných počítačů a jiné evidenční údaje (dodací listy SW a HW, faktury za SW a HW, předávací protokoly, specifikační listy atd.). Tyto informace jsou pak v různých formách dostupné z aplikační části grafického rozhraní komponenty *PCInfo desktop,* která se při každém svém spuštění připojuje k mateřské databázi *PCInfo server.*

3.2.2 PCInfo desktop

PCInfo desktop je grafické uživatelské rozhraní aplikace *PCInfo MagicEYE* a zpravidla se instaluje na počítač správce domény (administrátora). Může být přítomný i na stejném počítači - serveru, kde se nachází základní komponenta *PCInfo server. PCInfo desktop* je technicky možné nainstalovat na libovolný počet počítačů, pokud je to licenčně ošetřeno. Základní podmínkou pro spuštění *PCInfo desktop* je nepřetržitý přístup k SQL databázi aplikační části *PCInfo server.*

PCInfo desktop je ovládací sada nástrojů pro správu ostatních počítačů v síti, na kterých chceme provádět audity. Aby to bylo možné, je třeba mít na všech uživatelských stanicích nainstalovanou třetí komponentu *PCInfo klient.*

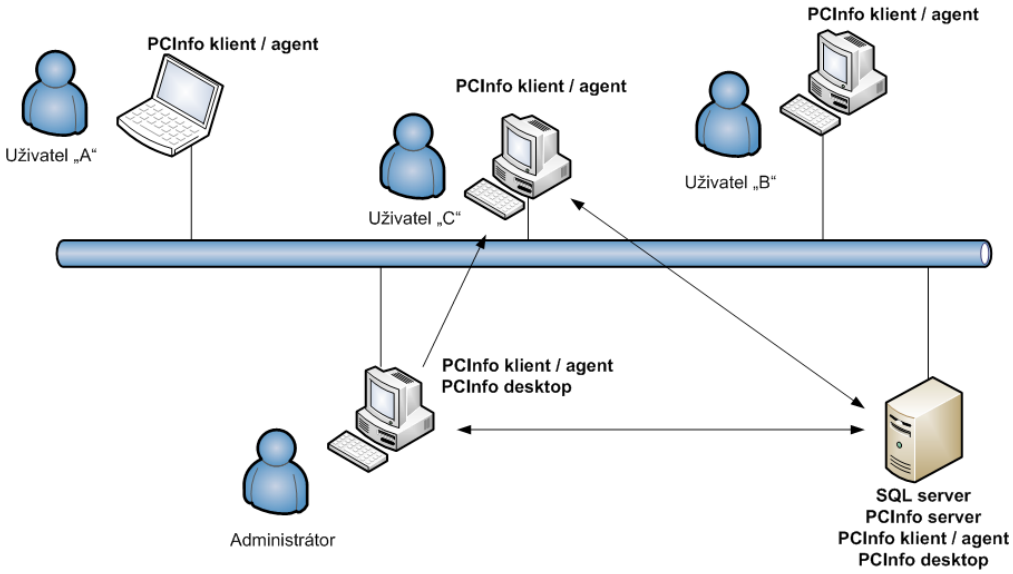
3.2.3 PCInfo klient a agent

PCInfo klient je sada nástrojů (včetně *VNC* serveru), která je kopírována z instalačního adresáře *PCInfo server* na lokální disky jednotlivých uživatelských stanic do adresáře ***PCInfo***, a to před spuštěním každého auditu počítače. Součástí je služba *PCInfo agent*, která umožňuje ovládat jednotlivé stanice sítě aplikací *PCInfo desktop.* Je tedy třeba, aby byla služba *PCInfo agent* přítomná a spuštěná na všech stanicích určených pro následnou komunikaci s komponentou *PCInfo server* a *PCInfo desktop*. Nejprve je potřeba *PCInfo klienta* nainstalovat, spustit *PCInfo agenta* a teprve poté je možné realizovat audit. Instalace aktuální verze sady souborů *PCInfo klient* by měla proběhnout před každým spuštěním auditu. Instaluje se automaticky pomocí originálního dávkového souboru ***PCInfo.bat*** z logon skriptu na všechny počítače a servery ve spravované síti. *PCInfo klient* podporuje tyto operační systémy:

- *MS – DOS* (všechny verze)
- *Windows 3.x, Windows 95/98/ME*
- *Windows NT/2000/XP*
- *Windows 2000 – 2008 Server*
- *Windows Vista, Windows 7*

Na lokálním disku počítače potřebuje minimálně 1,2 MB volného místa. Testování nainstalovaného software funguje i na platformách *IBM WinOS2* a *IBM PC DOS*. Hardware je dle údajů vývojářů aplikace *PCInfo MagicEYE* [14] možné testovat i na počítačích s operačním systémem *GNU/GPL Linux*. Modul *PCInfo klient* je tedy sada klientských programů sloužících k testování software a hardware na různých podporovaných platformách. Základem komponenty *PCInfo klient* je program ***PCinfo.exe***, který řídí požadované činnosti auditu na klientské stanici. Rozpozná také, zda byl audit spuštěn z přenosného média nebo ze sítě a podle toho odvíjí svoji další činnost.

Vztahy a role jednotlivých komponent aplikace *PCInfo MagicEYE* znázorňuje Obrázek 7.



Obrázek 7: Vztahy mezi komponentami PCInfoMagicEYE

3.2.4 Komunikace mezi komponentami PCInfo MagicEYE

Všechny počítače včetně serverů v celé síti zahrneme do evidenční databáze pro realizace softwarových auditů a vzdálené správy. Proto je nutné, aby byla komponenta *PCInfo klient* přítomna na všech spravovaných stanicích. Data o jednotlivých stanicích sbírá a ukládá databázová část aplikace *PCInfo server.* Administrátor má na počítači instalované grafické rozhraní *PCInfo desktop* pro správu všech stanic a serverů s *PCInfo* klienty.

Ukázkou je Obrázek 7: Administrátor vzdáleně identifikuje počítač uživatele „C“ a dá povel k instalaci *PCInfo klienta* z instalačních balíčků uložených na *PCInfo serveru.* Dále naplánuje nebo ihned spustí softwarový audit identifikovaného počítače. Data se po ukončení auditu automaticky uloží v zašifrovaném souboru do importní složky na *PCInfo server.* Tento šifrovaný soubor administrátor pomocí rozhraní *PCInfo desktop* nahraje do SQL databáze. S výsledky auditů nahraných v databázi *PCInfo serveru* lze pak pracovat pomocí SQL dotazů nebo generovat sestavy dle nastavených šablon přes rozhraní *PCInfo desktop.*

3.3 Možnosti užití aplikace PCInfo MagicEYE

3.3.1 Automatická detekce Hardware a Software

PCInfo klient je založen na automatické detekci hardware a software. Detekční metody jsou velmi přesné. *PCInfo klient* nevyžaduje manuální vyplňování mnoha informací o daném počítači, protože je jednoduše sám detekuje. Detekce vybavení počítačů nevyžaduje zdlouhavé obcházení uživatelů a osobní prohlídky jejich stanic. Požadované informace o softwaru a hardwaru auditovaných počítačů nám umožňuje získat konfigurovatelný generátor výstupních sestav obsažený v nástrojích grafického rozhraní *PCInfo desktop.*

3.3.2 Vyhodnocení softwarového auditu a jeho výstupy

Komplexní informace o SW a HW konfiguraci jsou prezentovány v jednoduché a přehledné formě. Je tak možné získat detailní seznam instalovaných aplikací, SW balíků a hardwarové konfigurace vybraného počítače na jedné obrazovce či vytištěné sestavě. Interní databáze *PCInfo MagicEYE* obsahuje více než 5000 registrovaných softwarových produktů celého světa.

Po provedeném auditu je aplikace schopna párovat informace registrovaných produktů v databázi *PCInfo MagicEYE* se zjištěnou skutečností na kontrolovaných počítačích. Může tak dle deklarovaných licenčních podmínek konkrétního výrobce SW upozornit, zda je daná aplikace či SW balík v organizaci užívaná legálně či nikoliv.

Kontroluje nesoulad mezi SW implicitně registrovaným v interní databázi *PCInfo MagicEYE*, skutečně instalovaným SW na počítačích a počtem povolených či zakoupených licencí v organizaci. Software, který ještě není registrovaný v interní databázi lze doplnit manuálně, aktualizací celého programu *PCInfo MagicEYE* nebo aktualizačním SQL skriptem. Komplexní výsledky auditů je možné zobrazovat v grafických přehledech na obrazovce počítače nebo vytisknout jako sestavu. Funkce generátoru tiskových sestav aplikační části *PCInfo desktop* umožňuje konfiguraci požadovaných výstupních položek auditu. Výstupní sestavy můžeme generovat za jednotlivé uživatele, počítače, nebo kompletně za celou organizaci.

Obrázek 8 zobrazuje část sestavy výsledku SW auditu za organizaci. V nástroji *„Evidence licencí“* rozhraní *PCInfo desktop* jsem pro názornou ukázku u aplikace *Microsoft Outlook 2003* zaregistroval počet 28 zakoupených licencí. U jiných SW produktů jsem licence neregistroval. Výsledky neregistrovaného software jsou v „červených záporných číslech“. V sestavě je software uveden jako rozdíl povoleného a nalezeného, čili jako nelegální, nepovolený nebo nekoncepční.

Nalezené programy Strana: 1

pro Finanční úřad v Moravské Třebové 10.2.2010

Jméno výrobce / Jméno programu	Popis	Verze	Zakoupeno	Nalezeno	Rozdíl
Adobe					
Acrobat Reader32				30	-30
Installation Acrobat Reader32 EN		4.05		1	-1
Microsoft Corp. - Office					
Access 2000 OEM/Installation				1	-1
Excel 2000				27	-27
Excel 2000 OEM/Installation				1	-1
FrontPage 2000 OEM/Installation				1	-1
Outlook 2000 OEM/Installation				1	-1
PowerPoint 2000				27	-27
PowerPoint 2000 OEM/Installation				1	-1
Word 2000				27	-27
Word 2000 OEM/Installation				1	-1
Outlook 2003			28	27	1
Symantec Corporation					

Obrázek 8: Ukázka výstupu auditu PCInfo za celou organizaci

3.3.3 Nástroje pro IT managery

Aplikace *PCInfo MagicEYE* umožňuje připravit řadu forem výstupních informací o spravovaných počítačích a jejich vybavení pro potřeby analýzy aktuální situace IT v organizaci. Generování předávacích protokolů jednotlivých počítačů usnadňuje předávání zodpovědnosti uživateli za komplexní vybavení svěřené stanice. Velmi účinná je tato praxe u notoricky neukázněných uživatelů, kteří se nemohou ubránit nutkání, instalovat nebo kopírovat nepovolený SW na svěřenou pracovní výpočetní techniku.

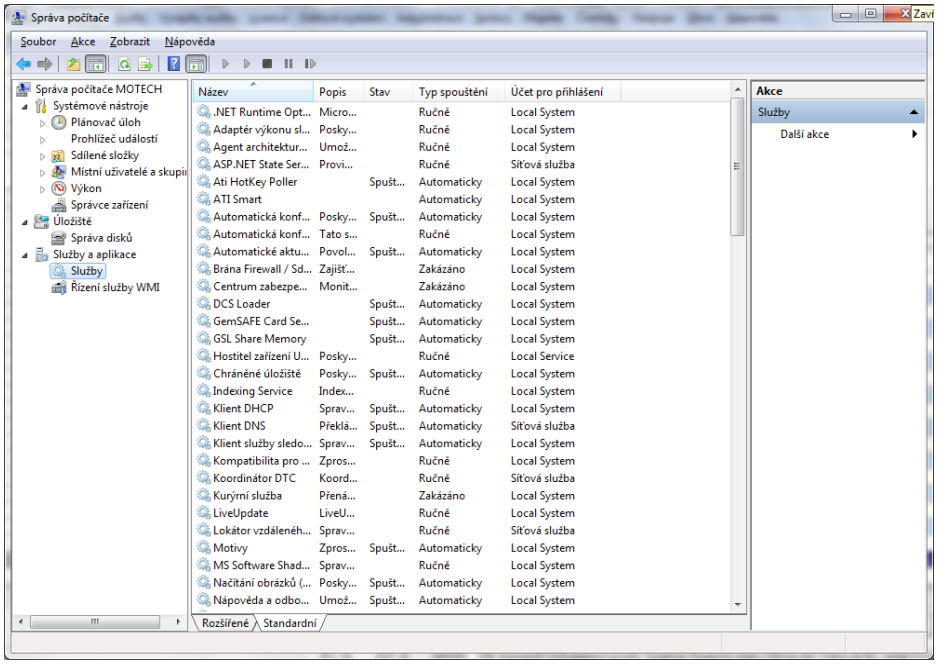
Specifikační listy počítačů umožňují rychle a pohodlně nahlížet na HW konfigurace jednotlivých stanic a podle požadavků vývojářů užívaného software vyhodnocovat, zda je HW konfigurace počítače dostačující nebo bude nutné provést upgrade. Nechybí agenda evidence pro hmotný a nehmotný majetek IT včetně správy faktur a účetních dokladů. Také evidence a kontrola počtu licencí zakoupeného a užívaného software, o které jsem se již zmiňoval .

3.3.4 Řídicí centrum sítě

Nástroj *„Řídící centrum sítě“* rozhraní *PCInfo desktop* poskytuje mnoho užitečných a praktických možností ke vzdálené správě počítačů v síti. Můžeme si zde načíst všechny počítače v doméně, pracovní skupině nebo dle rozsahu IP adres bez ohledu na to, zda mají či nemají instalovaného *PCInfo klienta*.

Vybrané počítače lze i vzdáleně vypínat či restartovat nebo můžeme posílat krátké textové zprávy přihlášeným uživatelům. Samozřejmostí je vzdálené otestování počítače „on demand", čili na žádost. Tato akce vyvolá SW audit on-line po síti v reálném čase kdykoliv to je zapotřebí. Týká se to i stanic, které doposud testovány nebyly a tudíž nejsou ani v databázi *PCInfo server*.

Řídící centrum sítě, jak ukazuje Obrázek 9, umožňuje počítače dálkově spravovat, řídit uživatelské účty, definovat místní zásady zabezpečení, ovládat služby a další. Nechybí funkce *„Vzdálená instalace programu"*. Pro tuto funkci je nutný účet s oprávněním uživatele skupiny *Administrators*. *PCInfo MagicEYE* poskytuje další možnou alternativu pro řešení problematiky vzdálených instalací programů.



Obrázek 9: Správa vzdálené stanice z PCInfo desktop

Problematika vzdálených instalací softwaru je více popsaná v praktické části diplomové práce (Kapitola 8.4.1; 8.4.2). Jsou zde uvedena dvě ukázková řešení v rámci spravované domény s adresářovou službou *Active Directory*.

3.3.5 Dálkové ovládání počítačů

PCInfo MagicEYE obsahuje nástroj *VNC* (Virtual Network Computing) pro dálkové ovládání. *VNC klient* umožňuje pomocí typu připojení klient-server a grafického rozhraní vzdáleně pracovat na jakémkoliv počítači v síti, na kterém rezidentně běží *VNC server*.

Na počítač uživatele lze přistupovat *VNC klientem*, který je integrovaný v sadě nástrojů rozhraní *PCInfo desktop.*

Můžeme tak provádět v omezené formě instalace software nebo jiné činnosti technické podpory uživatelů (např. navigace a pomoc při práci v uživatelských aplikacích, identifikace a odstranění příčin chybových hlášek, instalace tiskáren atd.). S uskutečněným připojením ke vzdálené ploše počítače uživatele může souběžně s tím probíhat i telefonická verbální komunikace.

3.3.6 Interní softwarový a hardwarový audit

Provádění softwarového auditu externí firmou s sebou přináší zvýšené náklady za služby. *PCInfo MagicEYE* dává možnost provádění interních hardwarový a softwarových auditů vlastními silami tak často, jak potřebujeme, bez jakýchkoliv dodatečných nákladů. Tento způsob je v konečném důsledku mnohem levnější a efektivnější řešení, zvláště pak u opakovaných či pravidelných periodických auditů. Nespornou výhodou také je, že se audit koná se bez přístupu cizích osob k výsledným informacím. Hlavní výhodou *PCInfo MagicEYE* je možnost hromadného testování stanic v síti v jeden okamžik bez nutnosti fyzického osobního přístupu k testovaným počítačům.

3.4 Rozšíření aplikace PCInfo MagicEYE

K rozšiřujícím modulům, které lze dodatečně dokoupit k základnímu balíku *PCInfo MagicEYE* patří *MagicMONITOR* pro sledování činnosti uživatelů a *MagicDESK* pro technickou podporu uživatelů. Nyní už k samotným programovým rozšířením *PCInfo MagicEYE.*

3.4.1 MagicMONITOR

Rozšiřující komponenta *MagicMONITOR* slouží k sledování aktivit uživatelů na definovaných počítačích. *MagicMONITOR* sleduje spouštěné aplikace, navštívené webové stránky, aktivní čas trávený v aplikaci či na internetu, počty úhozů na klávesnici, počty poklepání tlačítek myši, vytížení *CPU* a *RAM* počítače a další činnosti uživatele. *MagicMONITOR* je plně integrovatelný do systému *PCInfo MagicEYE*. Sbíraná data jsou ukládána v SQL databázi *PCInfo server.*

Na internetových stránkách [14] lze stáhnout zdarma 30-ti denní zkušební verzi této rozšiřující komponenty. Pro otestování funkcí programu, počítačů nebo některých „jinak aktivních“ pracovníků může být i časově omezená verze na jeden měsíc postačující. Pro větší rozmanitost a nezávislost na základním balíku *PCInfo MagicEYE* jsem zvolil jinou variantu komerčního software [15] určeného pro sledování aktivit uživatelů, než je rozšiřující komponenta *MagicMONITOR*. Více se prostředky pro sledování činnosti uživatelů budu zabývat v kapitole Kapitola 4.

3.4.2 MagicDESK

Intranetová webová aplikace *MagicDESK* je další rozšiřující komponentou aplikace *PCInfo MagicEYE*. Slouží k efektivnímu sledování a řízení uživatelských požadavků. *MagicDESK* umí spravovat požadavky uživatelů nejen z oblasti IT, ale také ostatních podnikových aktivit. Princip řešení spočívá v zadání uživatelského požadavku a následného přidělení kompetentnímu řešiteli na základě vybrané kategorie požadavku. Uživatelé tak mohou mít o řešených požadavcích neustálý přehled, ať už přes webové rozhraní nebo pomoci mailových zpráv, které je informují o stavu řešení svých požadavků. Postupem času tak lze vytvořit rozsáhlou databázi dotazů a řešení, čili „*znalostní bázi FAQ“,* která uživatelům umožňuje fulltextově vyhledávat již dříve řešené požadavky. Praktickým experimentem s podobným typem *„znalostní báze“* jsem na pracovišti s 26-ti uživateli ověřil, že takový typ pasívní podpory a svépomoci je malou skupinou pracovně přetížených uživatelů víceméně ignorován. Díky těmto zkušenostem jsem od praktického nasazení modulu *MagicDESK* v místních podmínkách našeho pracoviště upustil. Pro zajištění technické podpory uživatelů jsem se rozhodl vytvořit vlastní webovou *PHP* aplikaci *ServiceBook* určenou k zadávání servisních požadavků, jak bylo uvedeno v Kapitole 2.3.

Modul *MagicDESK* je vhodný pro nasazení do prostředí s pokročilými uživateli IT větších podniků či firem. Patří do rodiny systémů uživatelské podpory typu *HelpDesk.* Stejně jako *MagicMONITOR* je plně integrovatelný s databází hlavní části aplikace *PCInfo server* a spravovat ho lze pomocí rozhraní *PCInfo desktop*.

4 NÁSTROJE PRO SLEDOVÁNÍ ČINNOSTI UŽIVATELŮ

4.1 Morální hlediska sledování práce zaměstnanců na počítačích

Žádný zaměstnavatel si nemůže být zcela jist, že jeho zaměstnanci v práci opravdu vždy konají to, co je v náplni jejich pracovní smlouvy. Platit zaměstnance, který nemá na práci čas, znamená poškozovat organizaci a zprostředkovaně ostatní zaměstnance, kteří pracují za ty méně aktivní. Mezi každou organizací a jejím zaměstnancem je uzavřena pracovní smlouva. Tyto pracovní smlouvy jsou velmi rozdílné, ale všechny se shodují ve dvou bodech. Zaměstnavatel je povinen zaměstnanci platit mzdu a zaměstnanec je povinen vykonávat svěřenou práci. Kontrola zaměstnanců není jen morálním právem, ale také pracovní povinností nadřízeného pracovníka či manažera. Na kvalitě manažera pak závisí orientace spádového efektu jeho řízení. Zda bude mít vzestupnou či sestupnou tendenci. Pokud je to případ sestupné tendence, pak méně disciplinovaní zaměstnanci budou vykonávat méně práce a odvádět nevalné výsledky.

Neefektivní hospodaření se svěřenou výpočetní technikou je také energeticky náročné a s časem se navyšují náklady. Plnění kontrolní činnosti vedoucího pracovníka ovšem není vůbec jednoduché, pokud má takový manažer na starost početný tým zaměstnanců v rozlehlém prostoru (ve více budovách, městech apod.). Ne všichni zaměstnanci jsou vzorní a dostatečně motivovaní ke své práci. Mnoho zaměstnavatelů si tedy klade otázku: „Proč tedy platit za čas a práci, která nebyla odvedena?“ Takto vzniká poptávka po další kategorii SW aplikacích pro podrobné sledování, analyzování a srovnávání činnosti zaměstnanců. Takových SW produktů je v současné době k dispozici celá řada. Většinou jsou to komerční profesionální nástroje, které běží zcela skrytě na pozadí operačního systému sledované stanice. Zaznamenávají veškeré úkony, které sledovaný zaměstnanec na svěřeném pracovním počítači provádí. Shromažďují informace o časech a délkách trvání spuštění jednotlivých aplikací, konkrétní názvy otevřených dokumentů, předměty a příjemce mailové komunikace, adresy navštívených internetových stránek až po detaily, jako jsou znaky stisknutých kláves nebo počet kliknutí myší.

4.1.1 Etický pohled

Zda a do jaké míry je takové sledování zaměstnanců etické z hlediska ochrany soukromí a osobních údajů je velmi sporné. Pokud je sledování vykonávané v pracovní době zaměstnance a činnosti zaměstnance by měly být plně v souladu s jeho pracovními povinnostmi vyplývajícími z jeho pracovní smlouvy, lze to považovat za legitimní prostředek manažerské kontroly. Co však v případě, že má zaměstnanec pracovní přestávku, se kterou naloží tak, že si místo odpočinku na pracovním počítači vyřídí své soukromé platby elektronického bankovnictví nebo si přečte vlastní soukromou elektronickou poštu ze stránek svého „freemailového“ zprostředkovatele? Argumenty mají v tomto případě obě strany. Hodnotit však, na které straně je pravda mi nepřísluší. Osobně bych dal v podobném sporu prostor pro kompromisní řešení vycházejícího ze zdravého rozumu a moudré dohody mezi vedoucím pracovníkem a zaměstnancem, pokud je to vůbec možné.

4.2 Právní aspekty

Zákoník práce 262/2006 Sb. (s účinností od 1.1. 2007), přímo řeší oblasti tzv. zneužívání svěřených pracovních prostředků, a to včetně výpočetní techniky. Podívejme se tedy podrobně na některé paragrafy a analýzy litery zákona k podmínkám užívání nástrojů určených pro proces sledování činnosti zaměstnanců na svěřených pracovních počítačích.

4.2.1 Ochrana osobních práv zaměstnance

Ustanovení § 316 odst. 1 až 3 zákona 262/2006 Sb., zákoník práce:

OCHRANA MAJETKOVÝCH ZÁJMŮ ZAMĚSTNAVATELE A OCHRANA OSOBNÍCH PRÁV ZAMĚSTNANCE

§ 316

1. Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.
2. Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.

3. Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.

Analýza uvedeného:

Pak je tedy možné užívání monitorovacích programů, ale také žádoucí, aby byli zaměstnanci informováni o existenci a provozu monitorovacího systému na jejich počítačích.

4.2.2 Monitorování elektronické pošty, ochrana soukromí a osobních údajů

Stanovisko Úřadu pro ochranu osobních údajů č. 1/2003 s odkazem na Směrnici Evropského parlamentu a Rady 2002/58/ES je uvedeno v uvozovkách:

„...zaměstnavatel má právo sledovat u svých zaměstnanců dodržování pracovní doby a jejího využití. Pro výkon tohoto práva nemá zaměstnavatel právo sledovat, monitorovat a zpracovávat obsah korespondence svých zaměstnanců. Zaměstnavatel by případně mohl pouze sledovat počet emailů došlých a odeslaných u svých zaměstnanců a požadovat, aby své soukromé záležitosti v pracovní době a na pracovišti vyřizovali v přiměřené a více méně v nezbytné míře, neboť, jak bylo výše uvedeno, ani pracovněprávní vztah neodstraňuje právo na přiměřené soukromí zaměstnanců…“

Analýza uvedeného:

Monitorovací program tedy nesmí mít aktivní zabudované funkce a algoritmy pro zpracování, zachytávání a uchování obsahu korespondence sledovaného pracovníka. Může však sledovat jejich četnost a analyzovat, zda nedochází ke zneužívání služební elektronické poštovní schránky k soukromým účelům.

Ve stanovisku Úřadu pro ochranu osobních údajů je dále uvedeno:

„Z pohledu ochrany osobních údajů je však nutno mít na zřeteli ještě další otázku, a sice, zda při monitorování emailové pošty dochází ke zpracování osobních údajů. Pokud by nedocházelo ke zpracování osobních údajů, pak by ani kompetence Úřadu pro ochranu osobních údajů nebyla dána.“

Analýza uvedeného:

Monitorovací systémy nesmí zpracovávat osobní údaje ve smyslu zákona o ochraně osobních údajů. Mohou evidovat pouze jméno a příjmení, případně jeho telefon a email (pokud jsou zadány), název a IP adresu počítače sledovaného pracovníka. Osobní údaje za těchto podmínek tedy nemohou být zneužity.

4.2.3 Porušování tajemství dopravovaných zpráv

Ustanovení § 182 zákona 40/2009 Sb., trestního zákona (platného od 1. ledna 2010):

HLAVA II: TRESTNÉ ČINY PROTI SVOBODĚ A PRÁVŮM NA OCHRANU OSOBNOSTI, SOUKROMÍ A LISTOVNÍHO TAJEMSTVÍ.

§ 182 Porušení tajemství dopravovaných zpráv

1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího počítačová data, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo

b) takového tajemství využije.

3) Zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který

a) spáchá čin uvedený v odstavci 1 nebo 2,

b) jinému úmyslně umožní spáchat takový čin, nebo

c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem, bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti.

Analýza uvedeného:

Monitorovací systémy ke sledování činnosti zaměstnanců na svěřeném počítači nesmějí ve své funkční podstatě obsahovat aktivní algoritmy a funkce, které by svojí činností mohly porušovat tajemství dopravované zprávy. Nesmí tedy nahlížet do obsahu zpracovávaných dokumentů a zpráv ani jiným způsobem zachytávat, shromažďovat, pozměňovat popř. neautorizovaně rozesílat jejich data.

4.2.4 Zásah do soukromí a porušení listovního tajemství

Listina základních práv a svobod - Článek 10 odst. 2 a Článek 13:

Článek 10

2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a osobního života.

Článek 13

Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

Občanský zákoník č. 40/1964 Sb.:

§ 11

Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.

Analýza uvedeného:

V případě užití monitorovacího systému se nesmí jednat o neoprávněné zasahování do soukromého a osobního života sledovaného zaměstnance, ale o monitorování využitelnosti počítačové stanice, která má sloužit pro vykonávání práce určené zaměstnavatelem, efektivitě a četnosti využívání programových prostředků určených pro řešení pracovních úkolů.

4.3 Volba vhodného monitorovacího systému

Z komerčních produktů určených pro účely sledovaní vykonávané činnosti na počítači je možné použít zmíněné volitelné rozšíření *MagicMONITOR* aplikace *PCInfoMagicEYE* [14], dále například software *eDetektiv* [25] nebo monitorovací systém *Dozorce* od společnosti *Label Software s.r.o*. [15]. Pro potřeby diplomové práce jsem vybral a reálně nasadil komerční profesionální monitorovací systém *Dozorce*. Zaujal mě svým elegantním provedením, minimálními nároky na systémové prostředky hostujícího počítače a širokou paletou nastavení pro různé typy sledování. Je možné ho nasadit lokálně jen na jednu určenou stanici nebo může být instalovaný na více počítačích a komunikovat mezi sebou typem spojeni klient-server. Dává možnost vzdálené tiché instalace, dálkového sběru dat a jejich vyhodnocení mimo sledovanou stanici. Dále pak možnost pravidelného odesílání nasbíraných dat emailem, pokud je počítač připojený k Internetu.

Program má intuitivní ovládání, minimálními nároky na systémové prostředky a je nesnadno odhalitelný (dokonce i v operačním systému *Windows Vista a Windows 7* při spuštěné službě ***Řízení uživatelských účtů*** se *Dozorce* chová naprosto diskrétně).

V praktické části diplomové práce uvedu možné alternativy monitorovacích programů z oblasti volně dostupného freeware. Zajímavým poznatkem praktické části diplomové práce je, že program (viz Kapitola 8.1), který primárně není určený pro účely sledování práce uživatelů (zaměstnanců), a tudíž není k tomuto účelu cíleně naprogramován, může být při specifickém nastavení parametrů svých funkci využitý jako celkem spolehlivý špionážní software. Jinak „nevinná“ aplikace takto účelově zneužitá může svého iniciátora velmi snadno dostat svými aktivitami do rozporu se zákonným ustanovením uvedeným v kapitole 4.2.3 a 4.2.4. Více informací a porovnání programů určených ke sledování činnosti zaměstnanců, včetně doporučení pro korektní nasazení z hlediska výše uvedené analýzy je uvedeno v praktické části diplomové práce.

5 BEZPEČNOST UŽIVATELSKÝCH A PROVOZNÍCH DAT

5.1 Ochrana dat před jejich ztrátou a poškozením

Se vzdálenou správou počítačů také přímo i nepřímo souvisí zajištění datové bezpečnosti (zálohy a archivace) a zabezpečení dat proti jejich zneužití v případě úniku nebo ztráty. Oblast zabezpečení dat se v současné době stává samostatnou IT disciplínou. Nejčastější a účinnou prevencí před případným únikem a zneužitím informací datových formátů je jejich efektivní šifrování v reálném čase. Zvláště pak na přenosných médiích (LAN, Wi-Fi, flash disky) a pracovních noteboocích. Zde se však budu dále zabývat pouze oblastí datové bezpečnosti, tj. zálohováním a archivacemi, čili zajištěním persistence a dostupnosti uživatelských dat pro případ funkčního selhání primárního datového úložiště fyzického média.

Téměř vždy mají uživatelé na počítačích uložena pracovní data, která jsou pro samotné zaměstnance, potažmo pro celý podnik více či méně důležitá. Mnohdy obsahují velmi citlivé údaje (osobní data, know-how podniku atd.). Z toho důvodu je vhodné vytvořit koncepci zálohování a zálohovací plán pro počítače a servery v celé organizaci. Obecně řečeno, kromě interně prováděných on-line záloh formou jejich replikace a komprimace na jiná úložná média v síti, je také doporučeno tyto zálohy dále duplikovat na off-line média, a to nejlépe ve dvou vyhotoveních. Jako úložná média lze volit magnetické pásky, optická média *DVD,* externí diskové jednoty a další.

Datová archivační média je dobré fyzicky uchovávat v jiné místnosti, budově či bance v přiměřeném teplotním a vlhkostním klimatu. Tímto opatřením zamezíme totálnímu zničení a ztrátě dat v případě živelné pohromy v místě organizace. K zabezpečení archivovaných dat na přenosných médiích je možné užívat různé komprimační metody s ochranou dat přístupovým heslem, symetrické a asymetrické šifrovací algoritmy, čipové karty či biometrické technologie.

5.1.1 Obecné požadavky na zálohovací software

Výběr vhodné zálohovací aplikace a následně konfigurace zálohovacího systému pro celou doménu nebo pracovní skupinu je zásadní věc pro spolehlivé zabezpečení důležitých systémových a uživatelských dat.

Pro výběr vhodného software zvažujeme zejména splnění následujících kritérií :

- Zajištění důvěryhodné zálohy s možností snadné obnovy.
- Centrální administrace distribuované aplikace a vyrozumívání o událostech.
- Možnost zálohování používaných aplikací, otevřených souborů a databází.
- Možnost rychlé a snadné obnovy ze záloh v případě zhroucení systému nebo havárie pevného disku.
- Široká podpora operačních systémů, užívaného hardware s možností použití specializovaných technologií a zařízení *(SAN, NAS, DAS, cluster atd.)*.

Systém pro zálohování dat by měl splňovat určitá obecná kritéria, která jsou pro jeho funkci a správu nezbytná. Vysoká spolehlivost, přehlednost, intuitivní ovládání, zpracování grafického uživatelského rozhraní s možností vzdálené správy hlavního serveru a distribuovaných klientů aplikace jsou nesporně důležitými vlastnostmi moderního zálohovacího software.

- Přehledné grafické rozhraní - umožňuje snadnou orientaci v programu, rychlou konfiguraci a správu běžných zálohovacích úkolů (intuitivní ovládání podpořené nápovědou a navigačními průvodci).
- Modularita a rozšiřitelnost - je třeba chránit data nejen na lokálním serveru, ale i data ostatních počítačů v rámci lokální či vzdálené sítě.
- Centrální administrace systému - umožňuje nejen sledování průběhu zálohování a prohlížení logů, ale i vzdálenou konfiguraci zálohovacích úloh.

5.1.2 Analýza vlastností zálohovacího softwaru

Než zvolíme a zakoupíme konkrétní zálohovací software, je dobré položit si několik otázek týkajících se našich požadavků a najít na ně co nejpřesnější odpovědi. Podle toho zvážit, který nabízený software bude mít pro nasazení v našich podmínkách ty nejvhodnější vlastnosti. Otázky by měly být asi takového charakteru:

- Je možné užít datovou kompresi? Lze zvolit stupeň komprese? Je možné provádět zálohy dat i po síti? Probíhá komprese dat až na zálohovacím serveru nebo před přenosem na zálohovaném počítači? Je prioritou doba zálohování nebo objem přenášených a ukládaných dat?
- Umí aplikace provádět také inkrementální a diferenciální zálohy? Umí zálohovat otevřené soubory a databáze? Je možné vytvářet obrazy diskových jednotek? Lze pak z vytvořených obrazů disků spolehlivě a korektně jednotky obnovovat? Obsahuje aplikace pro obnovení diskové jednotky všechny potřebné ovladače hardwaru (zvláště řadiče disků a diskových polí)?
- Je program spolehlivý a důvěryhodný? Neobsahuje závažné chyby? Máme dostatek informací z referencí od ostatních uživatelů? Je určený a použitelný pro naši platformu? Jaké má nároky na systémové prostředky? Potřebuje speciální API?
- Má integrované algoritmy pro verifikaci a opravu chyb v zálohovaných datech? Jsou komprimované zálohy ve standardních formátech a lze je časem dekomprimovat bez zdrojové zálohovací aplikace?
- Obsahuje spolehlivé šifrovací algoritmy? Odesílá zálohovaná data z počítačů na server po síti otevřená nebo již šifrovaná? Jde o uznávanou a neprolomenou šifru?
- Jsou průběhy záloh zapisované do logů? Lze logy záloh odesílat emailem? Je možné aplikaci spravovat přes webové rozhraní? Má vlastní integrovaný webový server? Je zajištěna stálá technická podpora vývojářů a možnost provádění on-line programových aktualizací?
- Je možné zálohovací úlohy plánovat? Má plánovač speciální pokročilé funkce? Dokáže řídit priority zálohovacích úloh podle vytížení systémových prostředků zálohovaného počítače? Lze provádět synchronizace a replikace dat dle jejich změn v reálném čase? Je možné selektovat soubory a adresáře, které nebudou zahrnuty do výběru zálohovaných dat? Umožňuje aplikace před spuštěním zálohovací úlohy vypínat vybrané databázové služby, spuštěné aplikace s otevřenými soubory a po ukončení zálohování je opět spustit?

Otázek si můžeme položit celou řadu. Vše záleží na konkrétních požadavcích síťové infrastruktury. Naopak můžeme dojít k závěru, že není potřeba pořizovat robustní, certifikovaný a poměrně nákladný zálohovací systém. Mnohdy postačují celkem jednoduchá a přitom velmi spolehlivá řešení. Jsou nabízena na Internetu zcela volně jako freeware nebo pod licencí *Open Source*. U nekomerčních programů je však nutné počítat s rizikem nedostatečné nebo dokonce žádné podpory vývojářů v případě chyb nebo nekorektního chování zálohovací aplikace.

5.1.3 Výběr zálohovacího software

Z komerčních profesionálních nástrojů je velmi spolehlivý a stále vyvíjený software *Symantec Backup Exec*. V současné době je na trhu jeho aktuální verze *Symantec Backup Exec 2010* a přináší mnoho nového včetně speciální technologie tzv. *Granulární obnovení*. Nechybí možnost vytváření kompletních záloh systémových logických jednotek technologií *Inteligent Disaster Recovery*. Více o funkcích aplikace *Symantec Backup Exec* uvádím v praktické části diplomové práce v kapitole 9.1.

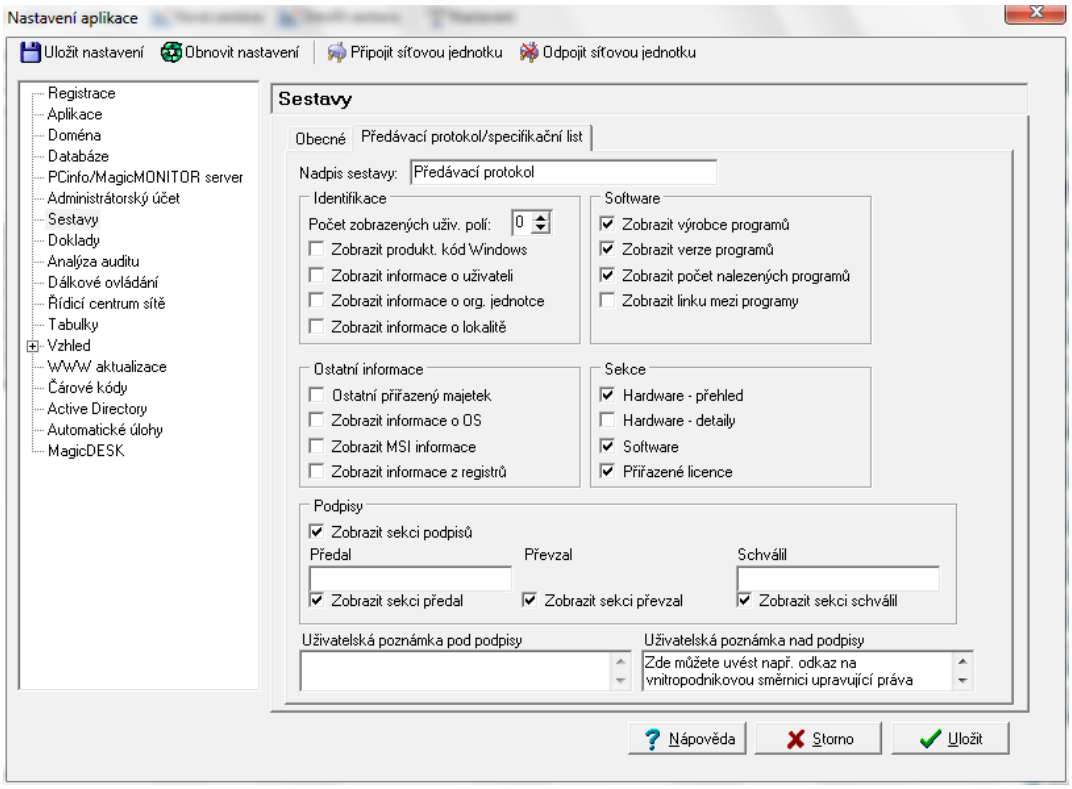
Pro vytváření bitových kopií pevných disků lze z oblasti volně dostupného software pod licencí *Open Source* použít aplikaci *EASEUS Todo Backup*. Zpracování této aplikace se velmi nápadně podobá komerčnímu produktu *Acronis True Image*. Chybí ji však mnoho pokročilých funkcí, kterými *Acronis True Image* disponuje. Z těch podstatných je to plánovač úloh, možnost zálohovat jednotlivé složky či soubory nebo obnova jednotlivých souborů či složek z bitové kopie diskové jednotky. Svým primárním účelem tvorby plných bitových kopií disků z prostředí Windows je *EASEUS Todo Backup* naprosto dostačující a relativně spolehlivý nástroj. V aktuální verzi programu *EASEUS Todo Backup 1.1* nechybí podpora operačního systému Windows 7 a všech dostupných serverových edicí Microsoft Windows. Otázkou však je, jak je to s podporou HW (diskových řadičů) u serverů v případě potřeby obnovení. Program *EASEUS Todo Backup 1.1* je součástí obsahu přiloženého CD.

II. PRAKTICKÁ ČÁST

6 REALIZACE SOFTWAROVÉHO AUDITU

6.1 Audit aplikací PCInfo MagicEYE

Po provedené instalaci a síťové konfiguraci všech potřebných komponent dle postupů instalačního manuálu *PCInfo MagicEYE* můžeme přistoupit k prozkoumání jednotlivých funkcí aplikace. Provedeme veškeré potřebné kroky, se kterými nás seznámí průvodce nastavení aplikace. Záložky možností nastavení zobrazuje Obrázek 10.



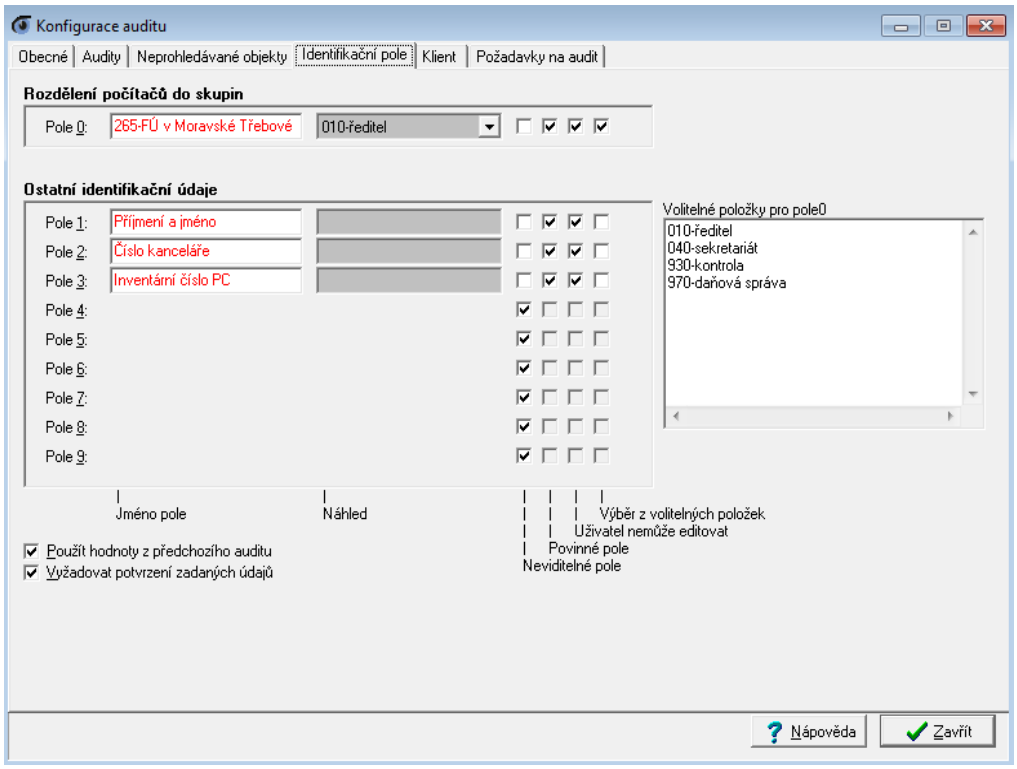
Obrázek 10: Nastavení aplikace PCInfo MagicEYE Desktop

6.1.1 Konfigurace softwarového auditu

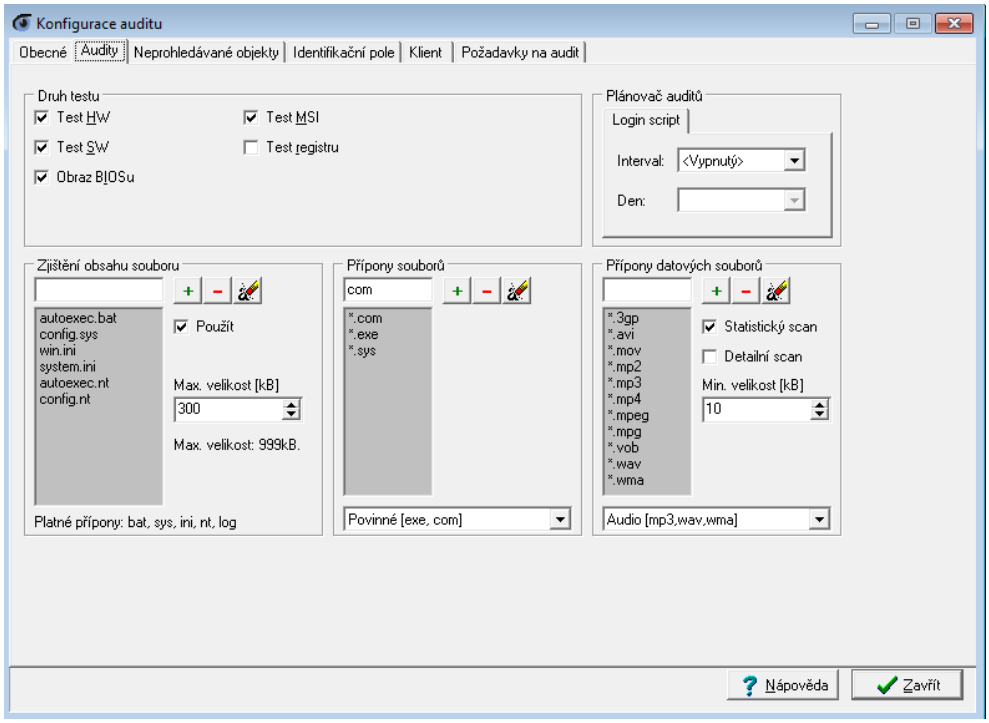
V rozhraní aplikace *PCInfo desktop* můžeme konfigurovat různé typy auditů:

- **Síťový individuální** – audit konkrétního počítače vybraného ze seznamu počítačů v síti nebo databáze *PCInfo sever.*
- **Síťový hromadný opakovaný** – provede otestování všech počítačů. Vygeneruje z databáze individuální pokyny k auditu všech dříve testovaných počítačů a upraví konfiguraci výchozího nastavení auditu pro kontrolu všech testovaných i netestovaných počítačů.

- **Médium** – dává možnost provádět audit na počítačích, které nejsou připojeny do sítě (test za pomoci přenosného média, zpravidla USB flash disk nebo disketa).
- **Síťový hromadný zaváděcí** – provede se na každém doposud netestovaném počítači, který není vedený v databázi *PCInfo server*. Podmínkou je zavedení inicializačního dávkového souboru pro spuštění instalace *PCInfo klienta*. V prostředí domény nejlépe do *logon skriptu*. Jedná se o speciální dávkový soubor ***PCInfo.bat***, který je součástí SW balíku *PCInfo MagicEYE* a je přítomný v instalačním adresáři *PCInfo serveru*. Dávka příkazů nakopíruje potřebné soubory *PCInfo klienta* na počítače jednotlivých uživatelů a spustí první zaváděcí audit. Uživatel musí při prvním prováděném auditu vyplnit identifikační údaje v nabízeném dialogovém okně. Konfiguraci položek nutných k vyplnění lze nadefinovat v *„Konfiguraci auditu“* v modulu *PCInfo desktop* – viz Obrázek 11. Stejně tak je vhodné nadefinovat „hloubku auditu“, čili co všechno je třeba v počítači otestovat – Obrázek 12.



Obrázek 11: Nastavení položek dialogového okna PCInfo auditu



Obrázek 12: Nastavení hloubky auditu

V konfiguraci auditu rovněž nastavíme, zda při instalaci *PCInfo klienta* povolíme nainstalovat službu serveru *VNC* pro dálkové ovládání. Dále nadefinujeme povolenou IP adresu počítače, ze kterého se bude provádět vzdálené připojení. Připojení *VNC* je možné také zabezpečit implicitním přístupovým heslem, které si uživatel může na své stanici v nastavení *VNC* serveru kdykoliv změnit a chránit se tak před nevyžádaným připojením.

6.1.2 Výsledky softwarového auditu

Konečné sestavy výsledných auditů – viz Příloha II. můžeme prohlížet na obrazovce PC nebo vytisknout. Kontrolu instalovaného software provedeme před tiskem předávacího protokolu a případné nesrovnalosti nalezeného nepovoleného software řešíme s uživateli osobně. Po provedené odinstalaci nepovolených programů opakujeme audit individuálně pouze na řešeném počítači. Opět provedeme kontrolu výsledné výstupní sestavy předávacího protokolu. Jakmile bude výsledek auditu vyhovovat veškerým licenčním politikám instalovaného a užívaného SW v organizaci, můžeme výsledné sestavy exportovat do datového souboru pro další zpracování mimo aplikaci *PCInfo MagicEYE* popř. vytisknout předávací protokoly či specifikační listy a nechat podepsat uživateli počítačů. Uživatelé tímto krokem přebírají zodpovědnost za následné odchylky v instalovaném softwaru a hardwaru na svěřené stanici do příštího prováděného auditu (např. po změně SW a HW konfigurace).

Databáze *PCInfo server* si vede podrobnou historii prováděných auditů v podobě kalendáře. Do konečných výstupních sestav promítá pouze výsledky poslední, aktuálně provedené kontroly (tj. nejmladší datum auditu).

6.1.3 Hodnocení PCInfo MagicEYE

Z testování, provozu a studie aplikace *PCInfo MagicEYE* jsem došel k závěru, že vyhovuje převážné většině požadavků pro komplexní správu výpočetní techniky a pro evidenci hmotného a nehmotného majetku oddělení IT. Dokáže rychle a spolehlivě identifikovat nepovolený nebo nekoncepční software a upozornit na případné nadlimitní instalace programů mimo rozsah zakoupených licencí. Sada integrovaných nástrojů umožňuje provádět vzdálené instalace programů, vzdálenou správu operačního systému a dálkově ovládat počítač pomocí vzdálené plochy aplikace *VNC*. Díky možnostem dalšího rozšíření komponentami *MagicMONITOR* a *MagicDESK* se sada nástrojů *PCInfo MagicEYE* stává komplexním a flexibilním softwarovým řešením pro správu majetku IT vhodným pro středně velké a velké organizace.

6.2 Audit aplikací WinAudit

WinAudit [20] je aplikace z oblasti nekomerčního freeware, která umožňuje provést detailní audit *HW* komponent počítače, ale také jeho SW vybavení a programových doplňků. Výhodou programu *WinAudit* je jednoduchost a snadná přenositelnost. Jde pouze o jediný programový soubor ***WinAudit.exe***, který se spustí na testovaném počítači. Audit lze provádět ručně z přenosných médií nebo vzdáleně po síti. Síťový audit lze spouštět z *logon skriptu*. Periodické spouštění auditu na jednotlivých stanicích lze realizovat pomocí „*Plánovače úloh Windows"*. Po spuštění prověřování je výslednou zprávou obrazovka s podrobnými údaji o instalovaném softwaru, periferiích, pamětích, procesoru, síťovém nastavení, spouštěných programech, procesech a mnoho dalších užitečných informací. Příloha III. obsahuje ukázky výstupů aplikace *WinAudit* .

Pro větší přehlednost mají jednotlivé kategorie komponent v levém rámci aplikace své záložky, takže pokud je třeba zjistit informace např. o operačním systému Windows a registračním ID jeho licence, verzi *BIOS*, typu procesoru nebo pevného disku, pak můžeme kliknout na odkaz požadované kategorie v záložkách seznamu. Výsledek auditu je možné exportovat do textového, *HTML*, či *XML* souboru, případně poslat v příloze emailem. *WinAudit* podporuje datové zdroje *ODBC,* takže výsledky auditu můžeme exportovat do existujících databází. Další výhodou je také česká lokalizace programu.

7 MONITOROVÁNÍ UŽIVATELSKÝCH AKTIVIT

7.1 Monitorovací systém Dozorce

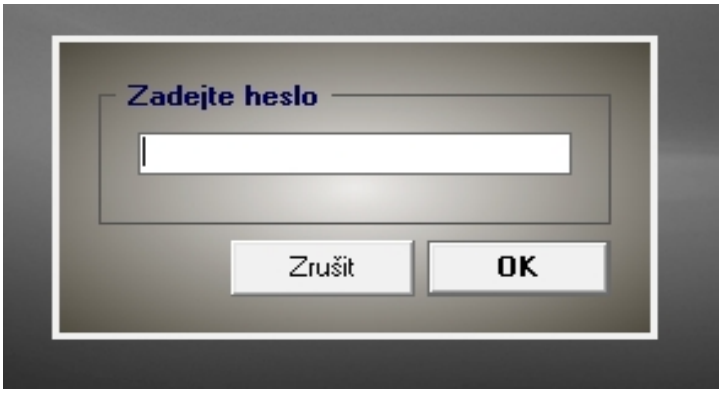
Nasazení monitorovacího systému *Dozorce* do běžného provozu je velmi jednoduché. Na stránkách výrobce [15] je dostupná ke stažení jednodenní zkušební verze tohoto programu. Na vyzkoušení funkcí to zcela postačuje. Zakoupením 2 licencí můžeme aplikaci nasadit mezi sebou ve spojení typu *klient-server*. Vývojáři navíc poskytují speciální program *RemRun* - viz Obrázek 14 pro vzdálenou síťovou, skrytou tichou instalaci na lokální síti, takže není třeba přímého fyzického přístupu ke stanici. Postačuje, aby byl uživatel přihlášený ke svému profilu Windows. Postup instalace je popsaný dále.

7.1.1 Instalace programu Dozorce

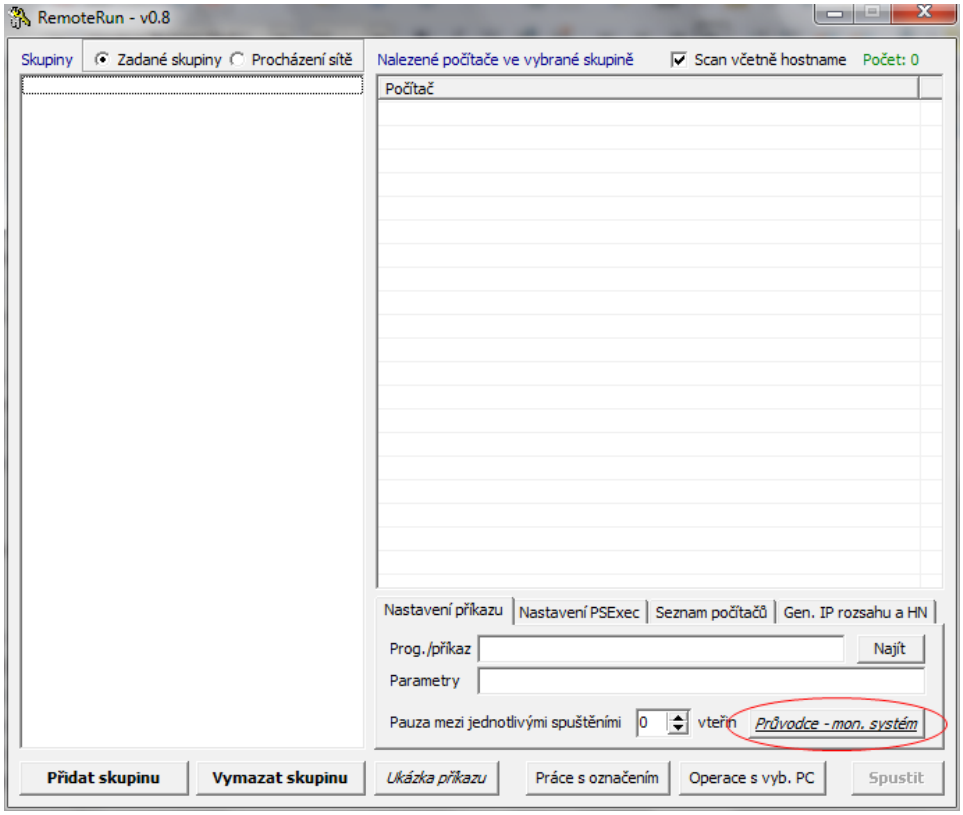
Na stanici administrátora (popř. manažera firmy) nainstalujeme první instanci programu (klienta). Ten při instalaci vyžaduje ověření platné licence na serveru výrobce. Po instalaci spustíme program *RemRun* a zvolíme IP adresu vzdálené stanice, na které nám poběží druhá instance programu v roli serveru, čili sledovaného počítače. Pokud je vzdálený počítač dostupný, vyzve nás program *RemRun* k zadání uživatele s oprávněním instalovat programy na vzdálenou stanici. Můžeme zvolit účet lokálního administrátora vzdálené stanice nebo doménového administrátora. Poté se *RemRun* postará o tichou instalaci programu na vzdálený počítač. Podotýkám, že uživatel vzdálené stanice musí být při této operaci přihlášený ke svému profilu ve Windows. Program *Dozorce* neběží jako služba, nýbrž jako rezidentní program spuštěný pro každého přihlášeného uživatele zvlášť. To se týká i následných vzdálených konfigurací programu či stahování nasbíraných dat.

Program se ihned po instalaci spustí a běží rezidentně na pozadí systému. Je možné ho vyvolat současným stiskem kláves CTRL+Shift+D – viz Obrázek 13. Tato kombinace kláves také jednoduše odhalí jeho přítomnost na PC. Zobrazí se přihlašovací tabulka pro zadání hesla do programu. Po instalaci je heslo prázdné, proto je ho třeba v konfiguraci programu zvolit. Program je na počítači nainstalovaný skrytě v systémovém adresáři Windows, jak ukazuje Obrázek 15. Lze ho ale odhalit ve správci běžících procesů jako proces ***msd.exe*** (**M**onitorovací **S**ystém **D**ozorce).

Aplikace se automaticky spustí ihned po přihlášení jakéhokoliv uživatele ke stanici. To je zajištěno klíčem v registrech – viz Obrázek 16.

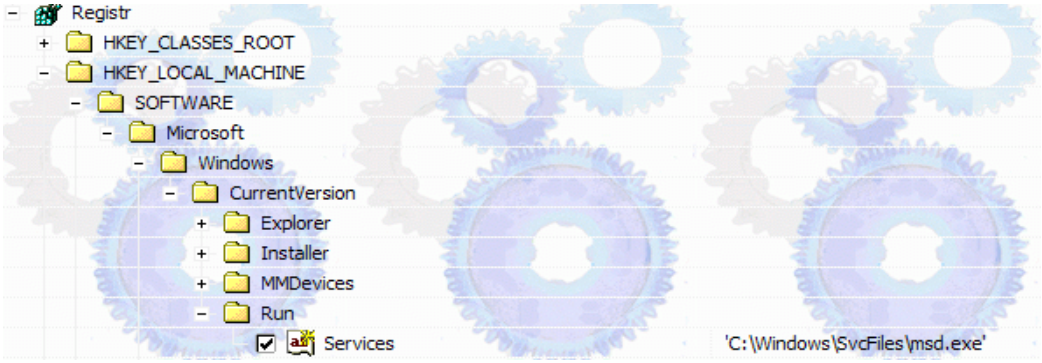


Obrázek 13: Okno přihlášení k programu Dozorce



Obrázek 14: Modul RemRun pro vzdálenou instalaci Dozorce

Obrázek 15: Skryté umístění programu Dozorce ve složce Windows



Obrázek 16: Klíč v registrech pro spuštění Dozorce po startu Windows

7.1.2 Nastavení a provoz programu Dozorce

Program je vhodné ihned po instalaci nakonfigurovat, a to na stanici administrátora či manažera a nastavení pak přenést i na vzdálenou sledovanou stanici. Jde především o nastavení hesla do programu a položek, které budeme chtít na stanici sledovat. Monitorovací systém *Dozorce* má opravdu široké možnosti sledování. Více obrázků k možnosti konfigurace programu jsem umístil do přílohy Příloha IV.

Velkou výhodou tohoto programu je možnost automatického zasílání výsledků sledování elektronickou poštou. Data jsou odesílaná v jediném souboru s příponou ***lgf***. Například soubor vygenerovaný pod názvem ***mf20100113.lgf*** má ve svém názvu datum, ke kterému se data obsažená v souboru vztahují. Možný je přenos dat i pomocí protokolu *FTP* jak je vidět na obrázku Obrázek 17.

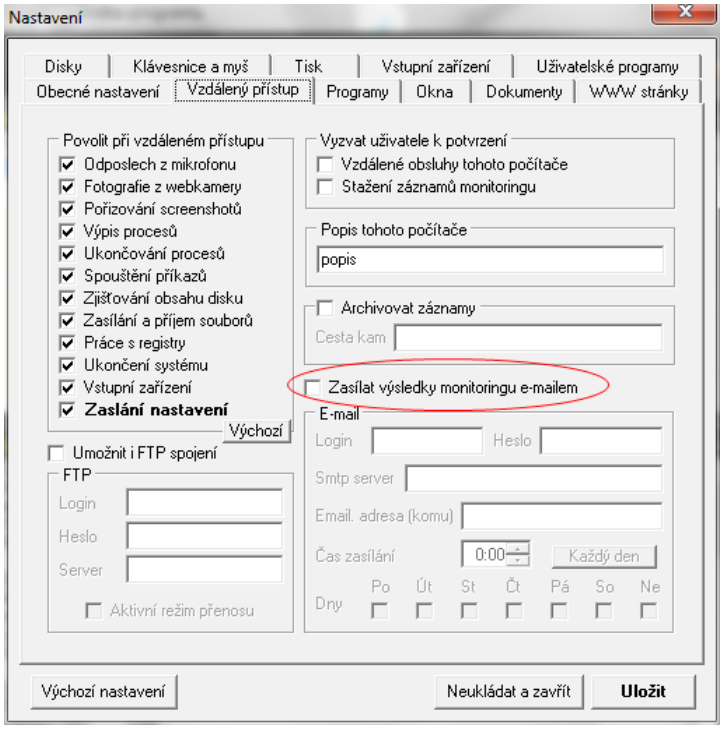
Dozorce umožňuje zaznamenávat otisky obrazovek z webkamery a zachytávat stream záznamu zvuku pořízeného z mikrofonního vstupu. Není pak problém pořizovat kompletní záznamy z telefonické komunikace přes Internet (*Skype, NetMeeting, GoogleTalk* apod.).

Program také umožňuje zachytávat znaky stisknutých kláves nebo zaznamenávat obsah schránky, použije-li uživatel kombinaci kláves **CTRL+C.**

Příloha IV. obsahuje bohatou kolekci obrázků z provozu aplikace *Dozorce.* Experimentální provoz monitorovacího systému *Dozorce* jsem uskutečnil po dohodě se sledovaným pracovníkem pouze pro potřeby této diplomové práce.

7.1.3 Sumarizace nasbíraných dat v grafech a tabulkách

Program *Dozorce* umí výsledky své činnosti přehledně zobrazit do tabulek a grafů. Statistické výstupy a výsledky z experimentálního sledování uvádím na následujících obrázcích: Obrázek 18, 19, 20, 21, 22, 23, 24.

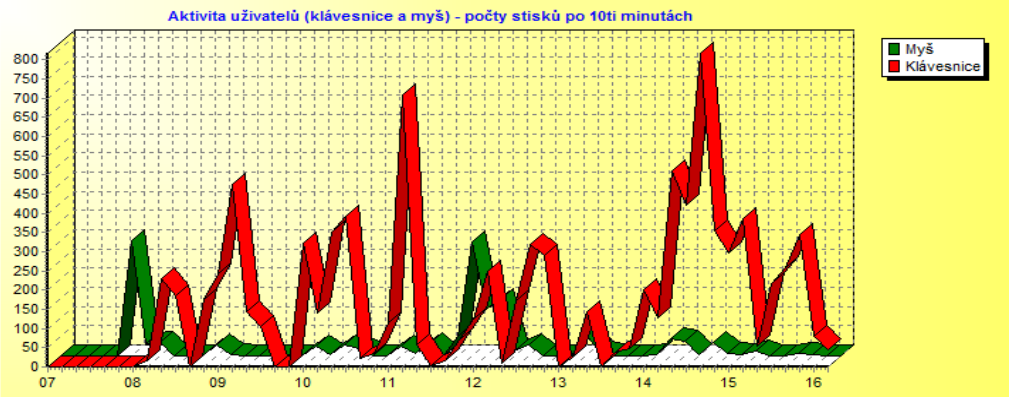


Obrázek 17: Nastavení odesílání dat v programu Dozorce

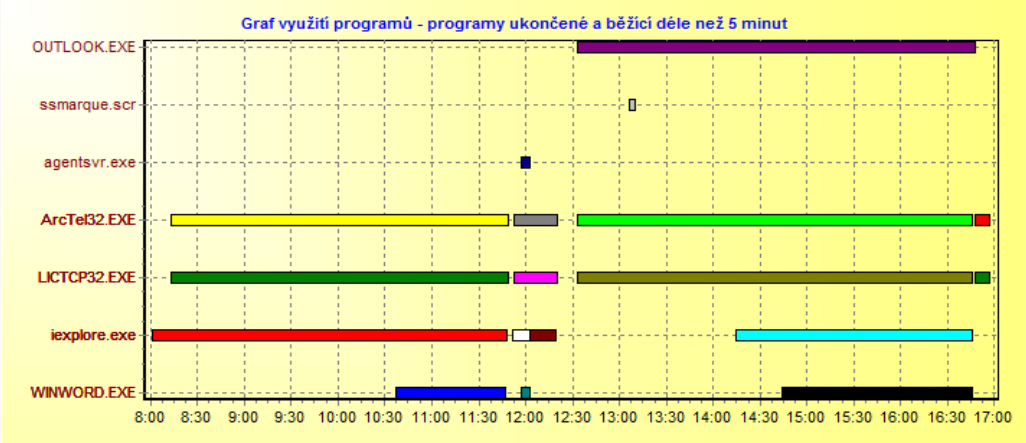
Za povšimnutí stojí fakt, v souvislosti s legislativou České republiky uvedenou v Kapitole 4, že program Dozorce umožňuje v konfiguraci zvolit takové nastavení, které dokáže pořizovat otisky obrazovky např. ze zobrazených poštovních zpráv nebo dokumentů – viz událost programu zvýrazněná na obrázku Obrázek 18, dále pak Příloha IV.

Čas	Událost	Detailní informace
7:54:23	Vytížení CPU	MHz: 30,8%
7:54:23	Paměť	Přehled: Fyzická: 76MB/502MB, Virtuální: 863MB/1227MB (84%)
7:54:32	Vytížení CPU	MHz: 71,9%
7:54:33	ScreenShot	Reakce na aktivní okno [pošta]
7:54:38	ScreenShot	Reakce na aktivní okno [Opakování: pošta]
7:54:42	Vytížení CPU	MHz: 42,2%
7:54:42	Paměť	Přehled: Fyzická: 56MB/502MB, Virtuální: 856MB/1227MB (88%)
7:54:43	ScreenShot	Reakce na aktivní okno [Opakování: pošta]
7:54:48	ScreenShot	Reakce na aktivní okno [Opakování: pošta]
7:54:52	Vytížení CPU	MHz: 46,6%
7:54:53	ScreenShot	Reakce na aktivní okno [Opakování: pošta]
7:54:58	ScreenShot	Reakce na aktivní okno [Opakování: pošta]
7:55:02	Vytížení CPU	MHz: 28,3%
7:55:02	Paměť	Přehled: Fyzická: 79MB/502MB, Virtuální: 851MB/1227MB (84%)
7:55:03	ScreenShot	Reakce na aktivní okno [Opakování: pošta]
7:55:05	ScreenShot	Reakce na aktivní okno [zpráv]
7:55:10	ScreenShot	Reakce na aktivní okno [Opakování: zpráv]
7:55:12	Vytížení CPU	MHz: 32,8%

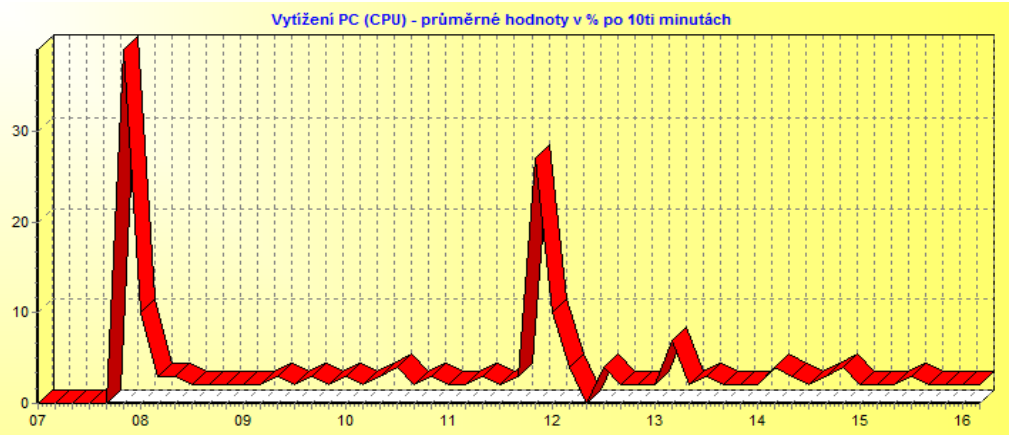
Obrázek 18: Záznam tabulky událostí v programu Dozorce



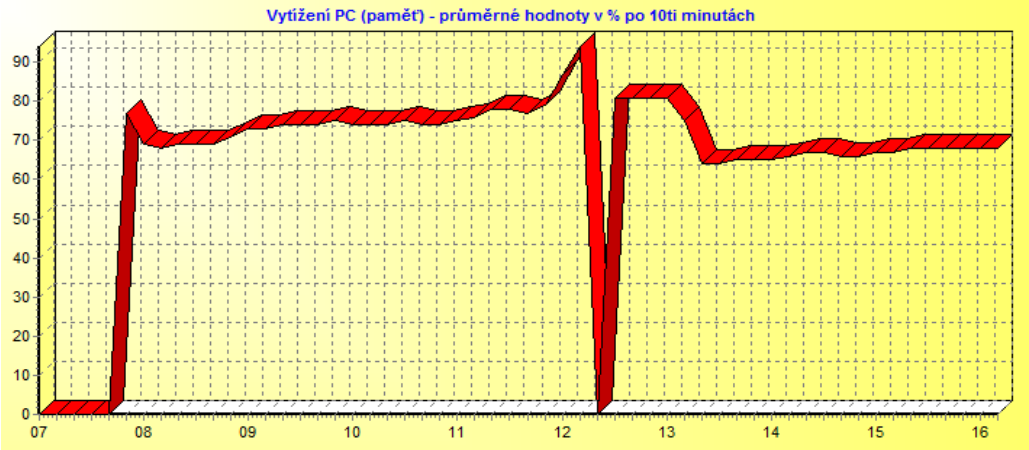
Obrázek 19: Graf aktivity uživatele v čase dle užití klávesnice a myši



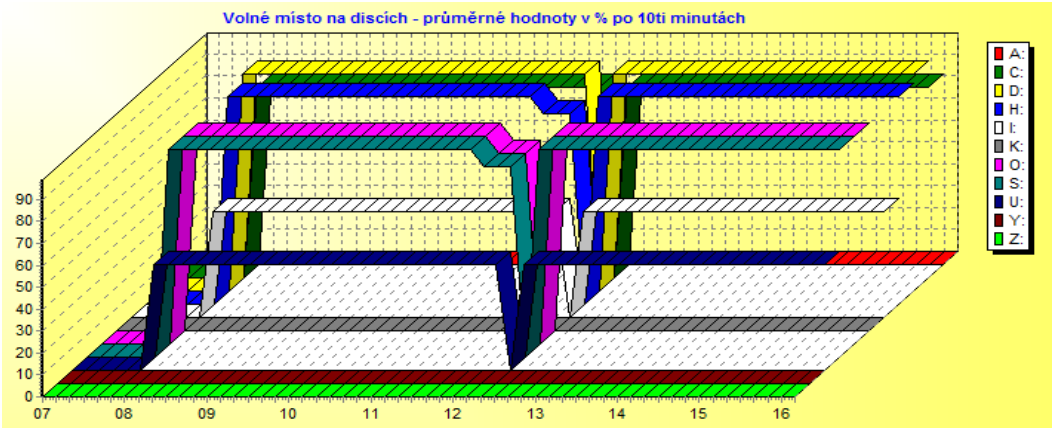
Obrázek 20: Graf aktivních a užitých programů během pracovní doby



Obrázek 21: Graf vytížení procesoru (počítače)



Obrázek 22: Graf vytížení operační paměti RAM



Obrázek 23: Využití kapacity připojených logických diskových jednotek

Statistika	Hodnota
Doba běhu Windows	8:49:41
Počet přihlášených uživatelů	2
Login přihlášených uživatelů	[redacted]
Počet nesprávných ukončení Windows	0
Počet startů Windows	3
Počet probuzení Windows	0
Počet ukončení Windows	3
Počet uspání Windows	0
Počet spuštěných jedinečných programů	19
Počet přepnutí na program	374
Počet zobrazených oken	130
Počet zobrazených WWW stránek	57
Počet vložených disků	6
Počet otevřených dokumentů	3
Počet tisků	21
Počet zaslaných stránek na tiskárny	11
Počet instalovaných programů	0
Počet odinstalovaných programů	0

Obrázek 24: Část tabulky se souhrnnými údaji monitoringu Dozorce

7.1.4 Hodnocení programu Dozorce

Monitorovací systém *Dozorce* [15] patří do skupiny „povedených“ komerčních programů určených pro sledování činnosti uživatelů. Spuštěný proces ***msd.exe*** zabírá v operační paměti pouze cca 630 kB. Průměrná velikost exportního souboru ***lgf*** s nasbíranými daty za 10-ti hodinovou pracovní dobu činí cca 15 MB (obsahuje cca 80 otisků obrazovek). Program *Dozorce* disponuje širokou paletou uživatelských nastavení pro požadovanou konfiguraci sledovaných aktivit. Program lze nastavit od sledování základních úkonů až po naprostou špionáž (zachytávání znaků hesel zadaných na klávesnici, snímání obrazovek otevřených dokumentů, webových stránek a elektronické pošty). Mezi pokročilé funkce monitorovacího systému *Dozorce* považuji zachytávání zvukové a obrazové komunikace zpracovávané na sledovaném počítači (*Skype, EyeBall, NetMeeting*).

Pořizovací cena tohoto software není vzhledem k jeho širokým možnostem nijak vysoká. Ovšem jeho praktické nasazení bych volil spíše do oblasti kriminalistiky, detektivních služeb a pro odhalovaní organizovaného zločinu. Na legální nasazení do podniků a firem pro sledování činnosti zaměstnanců je příliš kontroverzní. Většina předvoleb monitoringu zachází při svém praktickém použití za hranici zákona, pokud by byl program využitý do běžného procesu sledování činnosti zaměstnanců – viz Kapitola 4.

V následující kapitole zmíním alternativní aplikaci z oblasti freeware, která má naopak všechny předpoklady (alespoň z legislativního hlediska) pro zcela legitimní nasazení do procesu sledování činnosti zaměstnanců na svěřených pracovních stanicích.

7.2 Monitorovací program ManicTime

ManicTime je sledovací program primárně určený pro monitorování vlastních aktivit a doby strávené u počítače. Oblibu si tento program našel převážně u rodičů, kteří jej využívají ke sledování stráveného času a prováděných činností na počítačích u svých ratolestí. *ManicTime* zaznamenává čas aktivní i neaktivní činnosti počítače, spouštěné programové aplikace a odkazy navštívených webových stránek. Zaznamenané údaje průběžně ukládá do profilu přihlášeného uživatele a retrospektivně zobrazuje a barevně rozlišuje na časové ose. Události lze prohlížet v denních a týdenních grafech na obrazovce počítače – viz Obrázek 26, 27, 28.

ManicTime je k dispozici volně ke stažení na své domovské internetové stránce [21].

7.2.1 Instalace a nastavení programu ManicTime

Instalační průvodce programu *ManicTime* provede nejprve kontrolu přítomnosti knihoven API *Microsoft NET. Framework 3.5*. Pokud chybí, je nutné doinstalovat. Aplikace je po instalaci uživatelům zcela transparentní. Binární soubory a knihovny programu jsou implicitně umístěny v ***C:\Program Files\ManicTime***. Na rozdíl od monitorovacího systému *Dozorce* je možné provést standardní odinstalaci programu přes „*Správce programů Windows"*. O něco důkladněji je uschovaná souborová databáze ***ManicTime.sdf*** s ukládanými daty z procesu sledování. Ta je vnořená v adresářích profilů jednotlivých uživatelů s relativní cestou: ***..\LocalSetting\Finkit\ManicTime***.

Nastavení aplikace je triviální, jak ukazuje Obrázek 25. I když program postrádá českou lokalizaci, myslím, že jí zde není vůbec zapotřebí. Nasbíraná data ze souborové databáze je možné exportovat do textového souboru typu ***csv***.

7.2.2 Provoz aplikace ManicTime

Běh aplikace je transparentně signalizovaný kulatou barevnou ikonkou v systémové liště Windows. Kliknutím levým tlačítkem myši na ikonku vyvoláme okno aplikace. Pravým tlačítkem na ikonce zobrazíme kontextové menu s možností pozastavení monitoringu, například. pro účel pracovní přestávky sledovaného zaměstnance. Doba trvání přestávky bude ve výsledku monitoringu zobrazena jako časový rozdíl (pauza) mezi aktivním sledováním programu *ManicTime*.

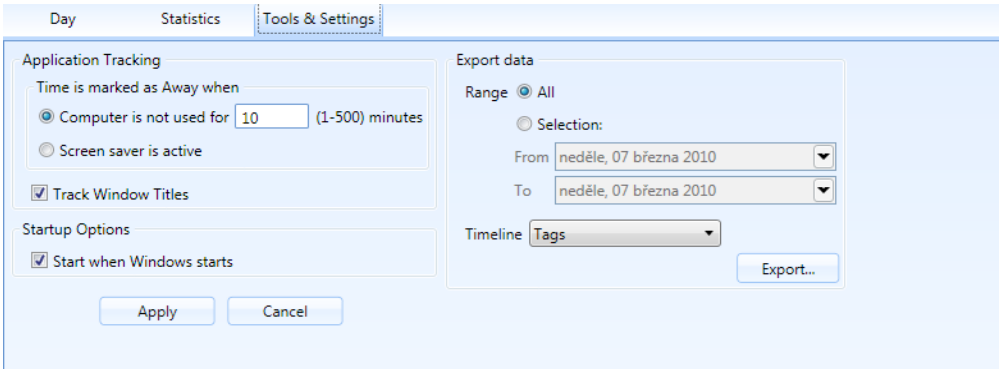
7.2.3 Hodnocení programu ManicTime

Podrobným studiem všech funkcí a dostupných možností programu jsem dospěl k názoru, že *ManicTime* není v konfliktu s Českou legislativou uvedenou v Kapitole 4. Je proto možné tuto aplikaci zcela legitimně užívat na klientských stanicích pro sledování činnosti zaměstnanců. Aplikace je shodou okolností navržena tak, aby splňovala všechna základní kritéria České legislativy pro nekonfliktní užívání k procesům sledování činnosti uživatelů na pracovních stanicích ve firmách a organizacích. Zde je shrnutí požadovaných vlastností legitimního monitorovacího systému:

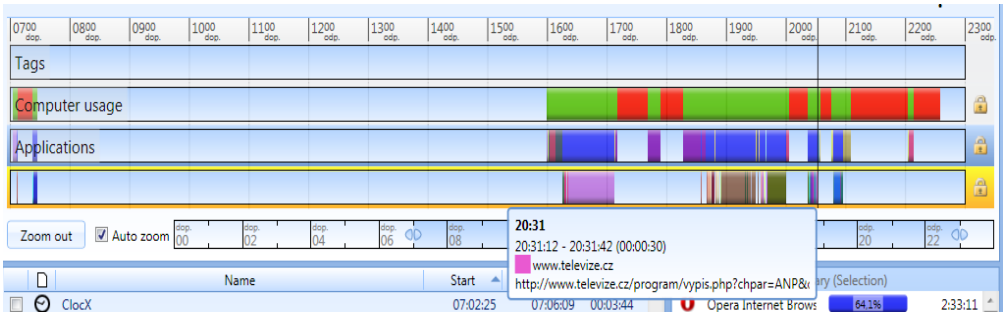
- Program běží na pozadí systému, ale má transparentní ikonu v systémové liště Windows. Informovaný uživatel může kdykoliv pozastavit proces sledování (např. během pracovní přestávky, pokud je taková dohoda se zaměstnavatelem uskutečněna). Čas a doba trvání pozastaveného monitoringu (stanovené přestávky) je také zaznamenána.

- Aplikace nezaznamenává ani jinak nezpracovává obsah otevřených dokumentů, webových stránek a poštovních zpráv. Zaznamenává pouze názvy dokumentů či názvy otevřených oken aplikací, adresy navštívených webových stránek, četnost, čas a délku trvání prováděných činností v jednotlivých aplikacích. Dále pak doby dílčí i celkové aktivní práce nebo nečinnosti počítače.
- Veškeré záznamy sledování ukládá pouze lokálně na sledované stanici, výsledky činnosti monitoringu a nasbíraná data nikde neputují po síti.
- Výsledné údaje monitoringu poskytují naprosto dostačující informace pro manažera či vedoucího pracovníka o efektivitě stráveného času a vykonávaných činnostech zaměstnance na svěřeném pracovním počítači během pracovní doby.

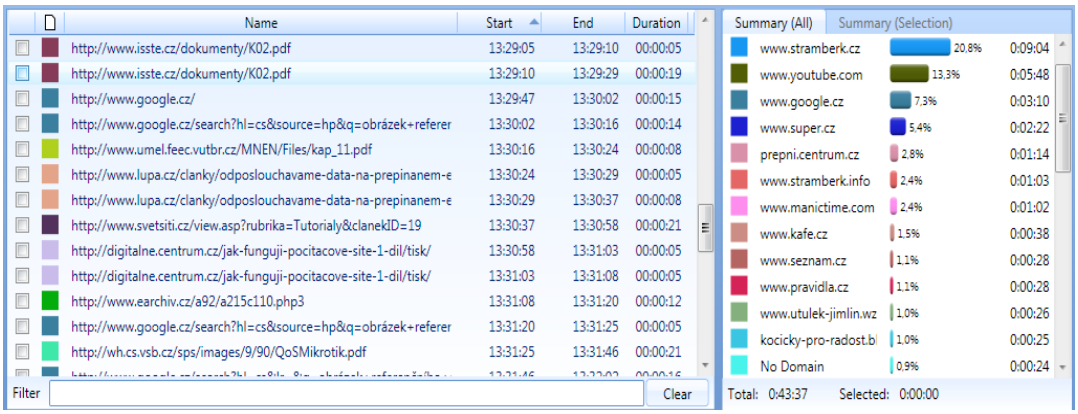
Nevýhodou procesu ***ManicTime.exe*** jsou příliš vysojé nároky na operační paměť. Hodnoty užívané fyzické operační paměti procesem ***ManicTime.exe*** během testovacího provozu kolísaly od 12 do 35 MB. Pomalé jsou také reakční doby programu, což má zřejmě z části na svědomí API *Microsoft NET. Framework*. Program rozhodně nedoporučuji používat na počítačích s nedostatkem volné kapacity fyzické operační paměti.



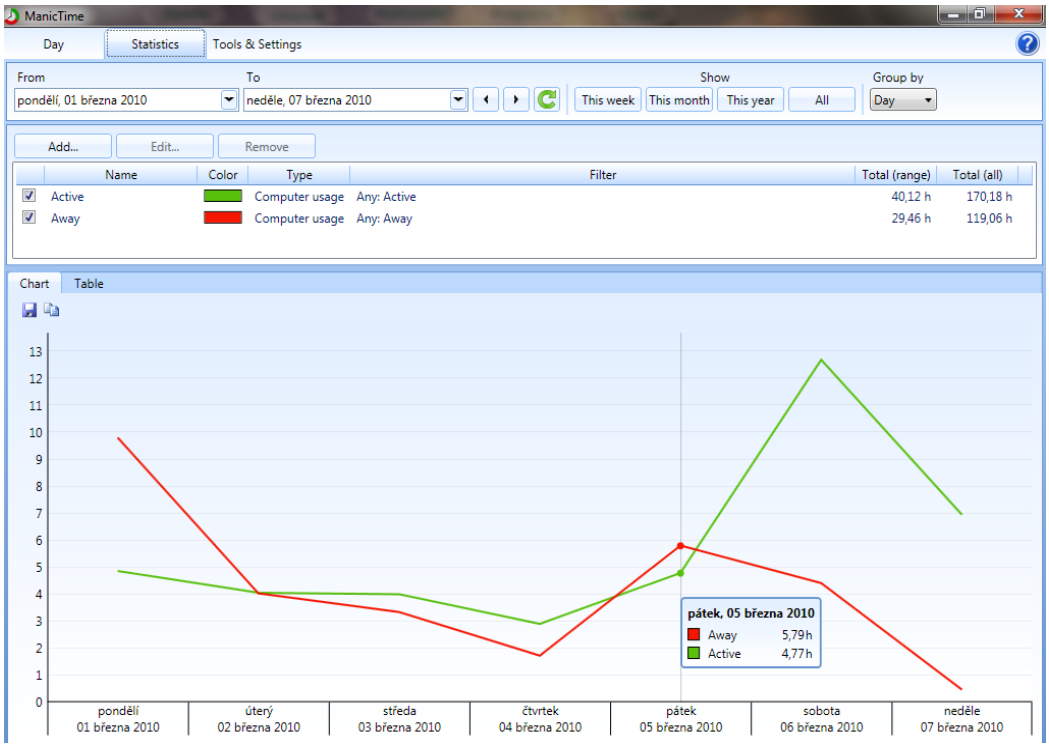
Obrázek 25: Možnosti nastavení v programu ManicTime



Obrázek 26: Zobrazení aktivit na časových osách ManicTime



Obrázek 27: Navštívené webové stránky a doba prohlížení



Obrázek 28: Týdenní graf činnosti a nečinnosti počítače

8 NÁSTROJE VZDÁLENÉ SPRÁVY

8.1 Speciální aplikace WinGrab

WinGrab verze 1.5.09 je program [19] z oblasti volně dostupného freeware, který je primárně určený k automatickému snímání obrazovek. Ty umí ukládat ve formátech: *BMP, JPEG, PNG* a *TIFF.*

Tento program velmi dobře poslouží jako nástroj pro bezobslužné samočinné pořizovaní snímků obrazovek na vybraném počítači nebo serveru. Je mnoho možností využití tohoto programu v oblasti administrátorské praxe. Jelikož je primárně určený jako pomůcka pro automatickou tvorbu otisků obrazovek, lze také specifickým nastavením uživatelských předvoleb dosáhnout snadné proměny programu ve špionážní nástroj. Tímto specifickým nastavením je možné docílit tiché spuštění programu po startu operačního systému, skrytý běh v pozadí systému a v libovolně nastaveném intervalu periodické snímkování obrazovky počítače. Snímky jsou ukládány do zvolené lokální složky nebo do sdílené složky jiného počítače na síti.

Princip činnosti *WinGrab* spočívá v tom, že aplikace má vlastní pokročilý plánovač, který řídí veškeré činnosti nastavené v uživatelských předvolbách. Není problém nastavit čas spuštění skenování, maximální počet snímků nebo dobu ukončení skenování a časový interval mezi snímkováním. Po splnění zadaného plánu může program ukončit pouze skenování obrazovek, sám sebe nebo celý operační systém. Je možné, aby snímkování probíhalo nepřetržitě po celou dobu běhu operačního systému Windows (u serverů to mohou být i celé týdny). Dosažením maximálního počtu uložených obrázků započne cyklické přepisování nejstarších snímků novými. Tím se zabrání přeplňování úložných kapacit.

8.2 Jednoduché řešení diagnostiky soketovou testovací funkcí

Implementace intranetového informačního portálu nebo servisní knihy může uživatelům sítě posloužit také jako diagnostický nástroj pro zjištění funkčnosti námi provozovaných služeb na serverech v doméně. Provozované síťové služby určuje číslo naslouchajících portů a IP adresa hostujícího stroje. Soketovou testovací funkci zavedeme do kódu našich webových stránek v jazyku PHP. Při načítání stránky zajistíme spuštění kódu a jednorázové spuštění soketové testovací funkce. Ta vyšle jeden testovací rámec na zadanou IP adresu a otestuje definovaný port dané služby, zda naslouchá nebo je uzavřený.

Návratová hodnota funkce ***fsockopen*** je uložena v našem případě do proměnné ***$adis***, která pomocí podmínky ***if-else*** zobrazí stav aplikace. V případě uzavřeného testovaného portu je návratová hodnota **0**.

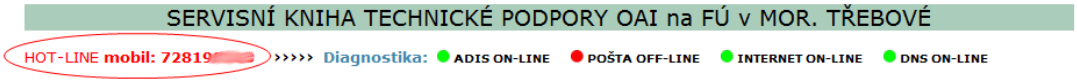
Ukázka příkladu soketové funkce implementované do kódu servisní knihy – viz Obrázek 4 vypadá následovně:

```
// POMOCNA FUNKCE PRO ZJISTENI  DOSTUPNOSTI  ADIS
function provoz_adis($stav) {
$adis = fsockopen ("NazevServeru", 80, $errno, $errstr, 0.5);
// adresa serveru, port WWW serveru, návratová hodnota chyby 1 a chyby 2,
// time-out pro načítání stránky ze serveru je 0.5 sekundy
if($adis) {
return $adis_stav = "<img src='./image/green.gif' alt='ADIS je přístupný' border='0'/>ADIS ON-LINE";
    } else  // vypisuje ON-LINE stav ADIS a zobrazí zelené návěští
return $adis_stav = "<img src='image/red.gif' alt='ADIS je nepřístupný' border='0'/>ADIS OFF-LINE";
}          //  jinak vypisuje OFF-LINE stav ADIS a zobrazí červené návěští
// KONEC FUNKCE PRO ZJIŠTĚNÍ STAVU ADIS
```

Princip uvedené ukázky kódu v jazyku PHP spočívá v testování portu 80, na zadané IP adrese nebo *DNS* názvu webového serveru informačního systému *ADIS*. Služba webového serveru je přímo závislá na provozu jádra aplikační části *ADIS* a na spuštěném databázovém stroji *Informix*.

Podobně lze testovat i jiné služby provozované na lokální síti jak ukazuje Obrázek 28. Pomocí soketové testovací funkce je možné do servisní knihy implementovat např. informaci o aktuálně platném telefonním čísle tzv. HOT-LINE pomoci. Princip spočívá v testování stanice Administrátora, u které je umístěný lokální HOT-LINE telefon. Stačí na tomto počítači zajistit, aby byl libovolný testovaný *TCP* port otevřený, kdykoliv se na počítači pracuje. V případě úsporného režimu počítače nebo běhu spořiče obrazovky či zcela vypnuté stanice bude testovaný port uzavřen. Na webové stránce servisní knihy se pak v době jejího otevření uživateli zobrazí právě dostupné telefonní číslo (stolní telefon pracoviště, pokud je na počítači administrátora vyvíjena aktivita, v jiném případě mobilní telefon) – viz porovnání zobrazení kontaktní informace o dostupném telefonním čísle mezi Obrázek 29 a Obrázek 30.

Obrázek 29: Nefunkční Microsoft Exchange server



Obrázek 30: Změna platného telefonu HOT-LINE v době nepřítomnosti

8.3 Problémy se spuštěním auditu PCInfo MagicEYE

V průběhu provozování aplikace *PCInfo MagicEYE* se mohou z neznámých příčin vyskytnout na některých uživatelských stanicích potíže se spuštěním auditu. *PCInfo agent* nereaguje na výzvy ke spuštění auditu ani při inicializaci aktualizace nové verze *PCInfo klienta*, ani na dálkově generované požadavky ze stanice s *PCInfo desktop*. V tomto případě je nutné provést kompletní odinstalaci *PCInfo klienta* včetně vymazání asociovaných klíčů systémového registru Windows na postižené stanici. Pro tento účel je vytvořený dávkový soubor ***PCI_Remove.bat*** [14]. Dávkový soubor je nutné spustit s oprávněním lokálního nebo doménového administrátora. Po jeho aplikaci a restartování operačního systému je možné opět inicializovat instalaci *PCInfo klienta*. Ihned po instalaci komponenty *PCInfo klienta* by mělo dojít ke spuštění auditu.

Dávky odinstalačních procedur ***PCI_Remove.bat*** jsou uvedeny v příloze Příloha V.

8.4 Logon skript pro potřeby vzdálené správy

Logon skript je dávkový soubor s definicemi příkazů, které se vykonají automaticky na počítači uživatele ihned po jeho přihlášení do domény ke svému uživatelskému účtu. Spouští se ze serveru doménového řadiče. Příkazy *logon skriptu* je možné definovat přímo pod službou *Active Directory* jako součást skupinových politik nebo vytvořit vlastní dávkový soubor s názvem ***user_logon.bat***. Ten můžeme definovat zvlášť pro každé oddělení či konkrétního uživatele. Ve vlastnostech jednotlivých účtů adresářové služby *Active Directory* ho můžeme explicitně definovat v záložce *„Spustit při přihlášení uživatele“*. *Logon skript* kromě příkazů pro mapování síťových logických diskových jednotek může obsahovat příkazy pro dálkové instalace, odinstalace, aktualizace, reinstalace a konfigurace uživatelských stanic.

Ukázku konkrétní aplikace dálkové hromadné instalace programu Adobe Reader spuštěné z *logon skriptu* uvedu v následující kapitole.

8.4.1 Instalace programu z logon skriptu

Velmi výhodné je *logon skript* užívat jako iniciátor k automatické dálkové instalaci či aktualizaci programů na spravovaných stanicích v síti. Uživatelé po přihlášení většinou nedisponují oprávněním pro instalace programů, proto je třeba zabezpečit spuštění instalátoru s oprávněním uživatele ve skupině *„Administrators“*. K tomuto účelu je dobré vytvořit speciální instalační doménový účet a zařadit ho do skupiny lokálních *„Administrators“* (ručně nebo pomocí služby *Active Directory*). Ten můžeme povolovat s časovým omezením na dobu platnosti prováděných automatických instalací inicializovaných z *logon skriptu*. Abychom mohli spustit instalátor programu z *logon skriptu* pod speciálním instalačním účtem, musíme použít příkazu Windows ***runas*** (spustit jako) a speciální utility ***sanur.exe,*** která vytvoří pipeline pro vložení hesla instalačního účtu zadaného přímo ve skriptu jako argument vstupního parametru příkazu ***runas***. Tím je zabezpečeno, že samotný uživatel nemusí zadávat ani znát informace o účtu s vyšším oprávněním včetně jeho hesla. I když je heslo v *logon skriptu* zadáno zcela transparentně, uživateli se nezobrazí, pokud před dávku zadáme příkaz ***echo OFF***. Utilitu ***sanur.exe*** umístíme do složky s instalačním programem. Není součástí systému Windows ani Resource Kit Tools Microsoft, takže je nutné si ji opatřit z webových stránek firmy Microsoft.

Zde je konkrétní ukázka dávky pro *logon skript* ke spuštění hromadné automatické instalace programu *Adobe Reader:*

```
@echo OFF
if exist c:\adobe930.test GOTO END
runas /user:DOMENA\SPECIALNI_UCET \\SERVER\disk$\SLOZKA\ADOBE9.30\AdbeRd~1.exe | sanur HESLO
copy /Y \\SERVER\disk$\SLOZKA\ADOBE9.30\adobe930.test c:\
:END
```

Za povšimnutí stojí užití jednoduchého testování přítomnosti souboru ***adobe930.test,*** který vytvoříme v instalační složce, libovolně pojmenujeme, nejlépe podle názvu a verze instalovaného programu a použijeme jako objekt pro testování již jednou spuštěné instalace. To nám zajistí, aby se při opětovném přihlášení uživatele instalace stejného programu již neopakovala. Tím, že je soubor ***adobe930.test*** po instalaci programu přítomný na disku počítače uživatele ještě není zaručeno, že instalace proběhla zcela korektně. V případě, že uživatel instalaci omylem či záměrně stornoval, musíme z jeho disku soubor ***adobe930.test*** ručně odstranit, aby se po opětovném přihlášení uživatele instalace znovu spustila.

Jakmile budou instalace provedeny na všech stanicích (kód ve skriptu ponecháme aktivní např. jeden týden), můžeme instalační příkazovou dávku z *logon skriptu* odstranit a speciální doménový účet z bezpečnostních důvodů zablokovat.

8.4.2 Instalace programu z Active Directory

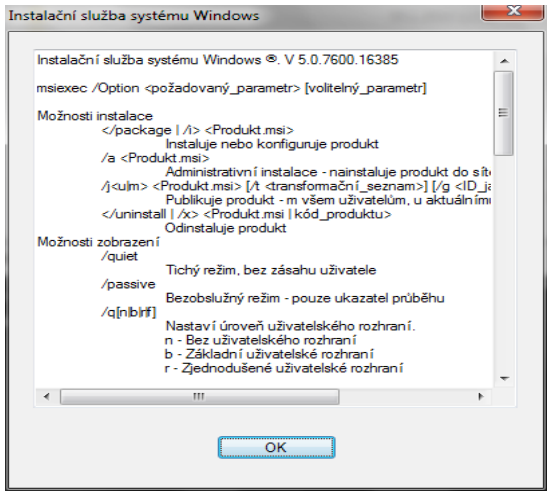
Hromadné instalace programů lze řídit i ze skupinových politik adresářové služby *Active Directory* [2]. Nutností však je použití balíčků s příponou ***msi*** tzv. ***Instalační služby Windows*** [3]. Balíčky tohoto formátu dovolují parametrizovat požadovaný průběh instalace. Typickým příkladem může být tichá a bezobslužná instalace na pozadí operačního systému bez zásahu uživatele. V případě, že bychom chtěli hojně využívat instalace programů pomocí adresářové služby *Active Directory*, existuje mnoho konverzních nástrojů, které umožňují běžný instalační soubor s příponou ***exe*** konvertovat do balíčku ***msi***. Nápovědu s instalačními parametry pro konkrétní balíček např. ***602voice.msi*** vyvoláme z příkazové řádky Windows takto:

```
602voice.msi /?
```

Zobrazí se okno s nápovědou ***Instalační služby Windows*** jak ukazuje Obrázek 31. Balíčky formátu ***msi*** jsou díky této parametrizaci mnohem výhodnější pro vzdálené instalace programů než běžné ***exe*** balíčky. Také je možné užit vzdálené instalace z ***msi*** balíčků za pomoci inicializace z *logon skriptu* nebo pomocí nástroje *„Řídící centrum → Vzdálená instalace“* z aplikačního prostředí *PCInfo desktop.*

Příkaz z *logon skriptu* pro tichou a bezobslužnou instalaci může vypadat následovně:

```
call \\CESTA_K_PROGRAMU\602voice.msi /quiet /passive
```



Obrázek 31: Okno nápovědy MSI

8.4.3 Importování klíčů systémového registru

Jak bylo uvedeno v kapitole 2.2, do dávky *logon skriptu* lze umístit i příkaz pro import klíčů systémového registru Windows ze souboru zpravidla s příponou ***reg***. Může to být již zmiňované nastavení výchozí webové stránky prohlížeče. Některé komerční aplikace čas od času vyžadují změnu licenčního čísla, které je v převážné většině případů importováno z programového uživatelského rozhraní do systémovém registru po jeho ručním zadání. Stejně tak můžeme zajišťovat importy klíčů pro spouštění programů po startu Windows nebo přihlášení uživatele, pro zastavování nebo spouštění systémových služeb atd. Zde je praktická ukázka dávky importu klíče registru z *logon skriptu* pro zajištění spouštění *VNC* programu po přihlášení uživatele. Připomínám, že dálkové ovládání *VNC* je součástí *PCInfo klienta*.

Příkaz z logon skriptu zajistí import klíče systémového registru:

```
rem ******** Nastavení spouštění VNC jako programu po přihlášení *********
 regedit /s \\CESTA_K_SOUBORU\VNC_StartUp.reg
```

Klíč v souboru *VNC_StartUp.reg* pak vypadá následovně:

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
 "WinVNC"="\"C:\\PCINFO\\WinVNC.exe\""
```

Následující klíč pak může explicitně zajistit nastavení domovské stránky v prohlížeči Internet Explorer (viz Kapitola 2.2) :

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"Start Page"="http://NazevInfoportalu"
"Default_Page_URL"="http://NazevInfoportalu"
```

8.5 Plánovač úloh Windows

Umožňuje při správě počítačů v síti konfigurovat a automaticky spouštět naplánované úlohy např. alternativní program ***WinAudit.exe*** pro pravidelné kontroly instalovaného softwaru - Kapitola 6.2. Bohaté využití nachází na serverech pro spouštění skriptů, aktualizací, údržby systému, zálohování dat atd. Dálkovou konfiguraci plánovače na stanicích uživatelů lze pohodlně provádět službou „*Vzdálená plocha Windows"*.

Jinou, avšak ne tak spolehlivou možností plánování je použití konzolového nástroje **s*chtasks*** [7]. Úlohu je možné konfigurovat vzdáleně z příkazové řádky pomocí služby ***telnet*** nebo opět pomocí *logon skriptu*. Uvedu ukázku příkladu, jak lze vzdáleně pomocí služby ***telnet*** a příkazu ***schtasks*** ručně naplánovat pravidelnou defragmentaci disku u konkrétního uživatele.

Předpokladem je přihlášení v příkazové řádce Windows službou ***telnet*** na počítači uživatele pod účtem jeho lokálního administrátora. Zadáním následujícího příkazu naplánuji pravidelné spouštění defragmentace diskové jednoty *C:* pod systémovým účtem (spustí se pravidelně každý týden v pátek v 18:00 hodin, pokud bude počítač zapnutý):

```
schtasks /create /RU SYSTEM /SC WEEKLY /D FRIDAY /TN „Defragmentace disku"
    /TR „C:\WINDOWS\SYSTEM32\defrag.exe c: " /ST 18:00:00
```

Podobným způsobem je možné naplánovat následující úlohu, která po dokončené defragmentaci zajistí vypnutí počítače příkazem ***shutdown*** s parametrem ***/s***. Při testování uvedených příkazů jsem se setkal s jazykovými rozdíly v argumentech parametrů u příkazu ***schtasks.*** Někde bylo třeba uvést české ekvivalenty jinde originální anglická slova. Záleželo to na konkrétní edici a verzi operačního systému Windows. Na některých stanicích s operačním systémem *Windows XP Professional SP3* se mi plánování úloh příkazem ***schtasks*** službou ***telnet*** vůbec nepodařilo. Velmi často se objevovalo hlášení typu **„Přístup byl odepřen".**

Podobným, ale starším plánovacím nástrojem je konzolová utilita ***at*** [7]. Definice plánu zmíněné defragmentace diskové jednotky *C:* by vypadala s příkazem ***at*** následovně:

```
at 6pm /every:FRIDAY „C:\WINDOWS\SYSTEM32\defrag.exe C: "
```

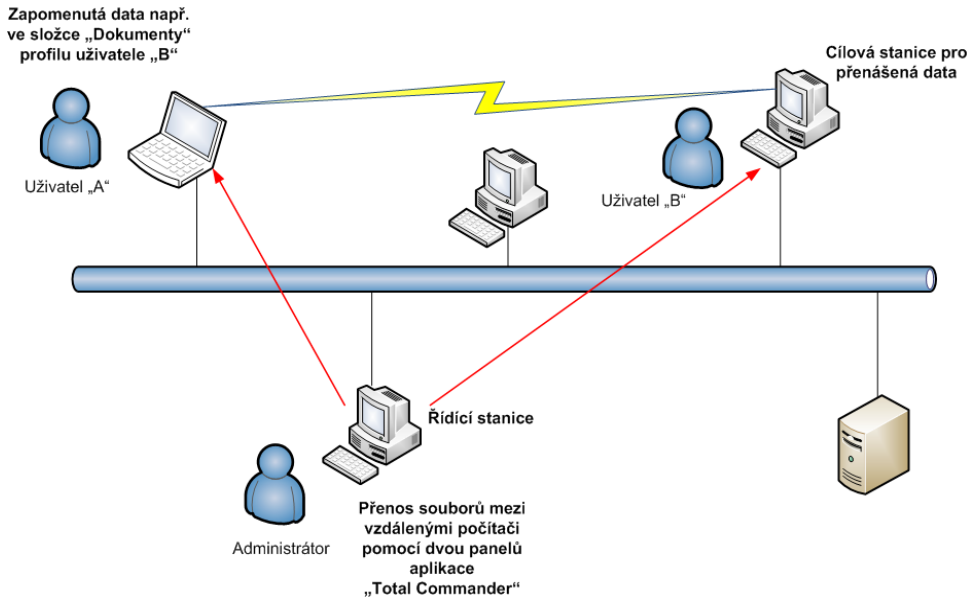
8.6 Total Commander

Kdo by neznal aplikaci *Total Commander*. Neocenitelný a nepostradatelný pomocník každého správce sítě. Oblibu si získal i u mnohých domácích uživatelů počítačů. Na Internetu je ke stažení mnoho generických programů, některé jsou komerční, jiné zdarma. Vyzkoušel jsem mnoho alternativních freeware programů, ale žádný z testovaných nezajišťuje takovou komplexitu funkcí jako *Total Commander*.

Pro potřeby dálkové správy počítačů se hodí pro operace se soubory a složkami v rámci celé spravované sítě. Dva panely *Total Commanderu* nám umožní provést z jednoho počítače pomocí *UNC* cest například tuto akci:

Uživatel „B“ se stěhuje z kanceláře jednoho konce budovy do kanceláře k počítači na druhém konci budovy. Na jeho místo přichází uživatel „A“. Aby mohl uživatel „B“ začít ihned pracovat, potřebuje překopírovat svá data nebo přenést svůj kompletní uživatelský profil z jedné stanice na druhou.

Pomocí *Total Commanderu* to lze vyřešit okamžitě a z jednoho místa, pokud jsou obě stanice spuštěné. Samozřejmě předpokládám, kvůli přístupovým právům, že program *Total Commander* je spuštěný pod účtem doménového administrátora, aby měl k uživatelským souborům plný přístup. Celou operaci znázorňuje Obrázek 32.



Obrázek 32: Vzdálené operace se soubory a složkami uživatelů

Pro operace se soubory a složkami v lokální síti nebo doméně považuji *Total Commander* za nepostradatelný nástroj. Pro vzdálené přenosy složek a souborů disponuje *FTP* klientem.

8.7 Nástroje PS Tools

Další zajímavou alternativou pro vzdálenou správu počítačů na síti je sada konzolových nástrojů *PSTools*. Pro podrobnější informace doporučuji zdroj [18]. Sada dvanácti nástrojů obsahuje tyto konzolové utility s pokročilou parametrizací:

PsExec	Spustí na vzdálené stanici proces nebo program
PsFile	Vypíše seznam otevřených souborů na vzdálené stanici
PsList	Vypíše seznam spuštěných programů a procesů na vzdálené stanici
PsPasswd	Umožní změnu hesla účtu na vzdálené stanici.
PsService	Zobrazí seznam aktivních služeb na vzdálené stanici.
PsShutdown	Umožní vypnutí nebo restartování vzdáleného počítače.
PsSuspend	Dokáže pozastavit a obnovit spuštěné procesy na vzdálené stanici.
PsGetSid	Zobrazí SID počítače nebo uživatele na vzdálené stanici.
PsInfo	Vypíše seznam informací o vzdáleném systému.
PsKill	Ukončí programy či procesy dle názvu nebo ID procesu.
PsLoggedOn	Vypíše přihlášené uživatele a uživatele využívající sdílené zdroje.
PsLogList	Vypíše záznamy z protokolu událostí (EventLog) vzdáleného počítače.

Jelikož se jedná o konzolové nebo také jinak „Command line“ nástroje, široké uplatnění najdou v dávkových souborech a skriptech. Textové výstupy procedur pak lze přesměrovat do souborů.

Jako příklad mohu uvést vzdálenou instalaci programu *Dozorce* (viz Kapitola 7.1.1) modulem *RemRun*, který pro tento účel využívá utilitu ***PSExec*** ze sady *PSTools*. Dalším příkladem může být případ, kdy potřebujeme zjistit, kdo z uživatelů nám blokuje otevřené programy a ***dll*** knihovny určité sdílené aplikace spouštěné ze serveru, kterou právě potřebujeme programově aktualizovat. K tomu účelu nám poslouží utilita ***PSList***. Z příkazové řádky zadáme:

```
PSList \\NAZEV_POCITACE >C:\vypis.txt
```

Výpis se v tomto případě neprovede na standardní výstup, kterým je obrazovka, ale do souboru ***vypis.txt***. Pokud takový dotaz posíláme z účtu doménového administrátora, nemusíme zadávat další parametry. V opačném případě je nutné zadat parametr ***-u Administrator*** a parametr ***-p*** za kterým následuje heslo.

Pro testování více počítačů v síti můžeme užít následující posloupnost příkazů z příkazového skriptu ***cmd*** s přírůstkovým zápisem výsledků do souboru ***vypis.txt:***

```
PSList \\POCITAC_1  >C:\vypis.txt
PSList \\POCITAC_2  >>C:\vypis.txt
PSList \\POCITAC_3  >>C:\vypis.txt
. . . . . .
PSList \\POCITAC_N  >>C:\vypis.txt
```

Po ukončení práce skriptu a naplnění souboru ***vypis.txt*** můžeme použít funkci *„Najít“* a vyhledat zadaný řetězec názvu programu např. v editoru *Notepad*.

Sada nástrojů *PSTools* je vhodným doplňkem k integrovaným příkazovým nástrojům, kterými oplývá operační systém Windows. Uvedu analogii příkazu ***TsKill*** k nástroji ***PsKill***. Obě tyto rutiny mají totožný cíl, a to ukončení činnosti definovaného procesu dle jeho názvu nebo ID. Zde je příklad užití příkazu ***TsKill*** v dávkovém souboru pro ukončení lokálně spuštěné aplikace web serveru *Vertrigo*. Jde o ukončení procesů *MySQL* serveru a *Apache* web serveru před provedením kompletní zálohy webových stránek včetně off-line zálohy souborů databáze:

```
@echo off
rem **********  Vypnuti aplikace WWW serveru  ************
tskill  /A  /V   v_mysqld
tskill  /A  /V   v_apache
tskill  /A  /V   Vertrigo
end
```

Příkaz lze užít i pro zrušení procesu na vzdálené stanici, obecná syntaxe zápisu je zde:

```
Tskill {ProcessID | ProcessName} [/server:ServerName] [{/id:SessionID | /a}] [/v]
```

ProcessID	ID procesu, který má být ukončený.
ProcessName	Název procesu, který má být ukončený.
/server: ServerName	Server, na kterém běží proces nebo ID procesu, výchozí je místní server.
/id: SessionID	Ukončí proces v rámci zadané relace.
/A	Ukončí proces ve všech relací.
/V	Zobrazí informace o prováděných činnostech.
/?	Zobrazí nápovědu k příkazu.

8.8 Skupina příkazů NET

Skupina příkazů ***NET*** je určena pro konzolové operace v sítích platformy Microsoft Windows buď ručním zadáním z příkazové řádky či jako spustitelných dávek příkazových skriptů.

Je součástí operačních systémů Windows a jednotlivé parciální funkce se mohou lišit v závislosti na konkrétní edici Windows. Ve skriptech pro vzdálenou správu je možné příkazy ***NET*** vhodně kombinovat se sadou nástrojů *PSTools*. Edice operačního systému *Windows 7 Professional* nabízí skupinu příkazů ***NET*** v této konfiguraci:

net accounts	Slouží k nastavení uživatelských účtů včetně doby platnosti hesla.
net computer	Přidá nebo ubere počítače z databáze doménového řadiče.
net config	Umožní konfiguraci služby *Server* a *Pracovní stanice*.
net continue	Nastartuje pozastavenou službu.
net file	Zobrazí a umožní ukončit sdílení otevřených souborů na serveru.
net group	Umožní práci se skupinami uživatelů – pouze na řadiči domény.
net help	Nápověda k příkazu *NET*.
net loclagroup	Umožní práci se skupinami lokálních uživatelů.
net pause	Pozastaví aktivní službu.
net session	Zobrazí všechna aktuální připojení k serveru nebo stanici.
net share	Vypíše názvy sdílených položek a prostředků.
net start	Spustí službu. Bez zadání názvu pouze vypíše všechny spuštěné.
net statistics	Vypíše statistiky služby *Server* a *Pracovní stanice*.
net stop	Zastaví službu systému Windows.
net time	Synchronizuje hodiny podle serveru doménového řadiče.
net use	Připojí sdílený prostředek (logickou síťovou jednotku).
net user	Vypíše uživatelské účty zadané stanice lokálně i na síti.
net view	Vypíše všechny aktuálně spuštěné stanice lokální sítě či domény.

V minulé kapitole jsem použil příkaz ***TSKill*** pro zrušení všech procesů www serveru *Vertrigo*. Pokud jde o procesy spouštěné rezidentně jako služby, můžeme je pouze pozastavit a poté opět spustit. Užití pozastavení a následného spuštění služby uvedu opět na příkladu pro potřeby zálohování databázových tabulek. V tomto případě využiji příkazu ***NET***. Ukázka kódu pro dávkový soubor k pozastavení a opětovnému spuštění služby ***Vertrigo MySQL*** serveru je následující:

Stop služby ***Vertrigo MySQL*** před zálohováním souborů databáze:

```
@echo off
rem ********** Stop služby MySQL server ************
net pause Vertrigo_MySQL
end
```

Start služby ***Vertrigo MySQL*** po zálohování souborů databáze:

```
@echo off
rem ********** Start služby MySQL server ************
net continue Vertrigo_MySQL
end
```

Z příkazové řádky můžeme také spouštět programy pro zálohování dat, které podporují „Command line“ s parametrizací. Jedním z nich je nástroj operačního systému Windows s názvem ***ntbackup.*** Obecně je známo jeho grafické rozhraní, avšak pro pokročilejší správu uživatelských dat a jejich zálohy po sítích je vhodné úžívat programový příkaz ***ntbackup*** z dávkových ***bat*** nebo příkazových ***cmd*** souborů. Velký nedostatek příkazu ***ntbackup,*** který jsem zaznamenal při jeho testování, je absence podpory práce s médii typu CD nebo DVD. V praxi se ale k zálohování dat častěji využívají pokročilejší nástroje třetích stran.

9 ZÁLOHOVÁNÍ A ARCHIVACE DAT

9.1 Symantec Backup Exec

Zálohovací systém *Symantec Backup Exec* je profesionálním zálohovacím řešením, které je certifikováno pro operační systémy platformy Microsoft Windows. Již několikaletý vývoj aplikace z něj vytvořil velmi výkonný, jednoduše ovladatelný a flexibilní nástroj pro řešení spolehlivého zálohování operačních systémů, kompletních aplikací, uživatelských dat a databází různých typů a platforem. Z praktického hlediska je vhodné *Symantec Backup Exec* nasadit jako distribuovaný systém klient-server. Je rozšiřitelný o speciální moduly pro zálohy dat z klientů na jiných platformách OS (Linux, MacOS atd.) případně z virtualizovaných systémů. Tyto speciální moduly nejsou standardně obsaženy v základním balíku *Symantec Backup Exec*, avšak e-shop [27] nabízí případným zájemcům možnost sestavení požadované vlastní distribuce pomocí webového konfigurátoru aplikace. Nemá význam zde jmenovat všechny vlastnosti *Symantec Backup Exec,* jejich podrobný výčet je dostupný na stránkách výrobce [27].

Za zmínku stojí ty podstatné, a pak také novinky, které jsou obsažené ve verzi *Symantec Backup Exec 2010:*

- *Inteligent Disaster Recovery* - modul řeší obnovu kompletního lokálního či vzdáleného systému včetně všech původních nastavení. Během obnovy je možné znovu definovat velikosti logických disků a ovladače síťových karet. Jde o obdobu zálohy a obnovy systému z bitové kopie (obrazu) svazku diskové jednotky.
- *Open File modul* - umožní pomocí cache na úrovni disku korektní zálohování exkluzivně zamčených nebo otevřených souborů.
- *Exchange Server Agent* - umožňuje kompletní on-line zálohu poštovního systému.
- *Microsoft Exchange Server* - agent umožní zálohovat jednotlivé mailboxy případně samostatné mailové zprávy.

Symantec Backup Exec 2010 nabízí mnohé novinky, jako například *„Granulární obnovení“* aplikací *Microsoft Exchange, MS SQL a Active Directory* v prostředích *VMware* a *Hyper-V.* Dále nabízí novou flexibilní metodu odstraňování duplicitních dat tzv. „deduplikaci“ pro zmenšování a konsolidaci prostředků vlastních datových úložišť [27].

Cena za jednu serverovou licenci základního balíku *Symantec Backup Exec 2010 Suite* činila na konci března 2010 částku 1 116 USD v e-shopu [27]. Základní balík je k dispozici ke stažení v časově omezené „Trial“ verzi pro praktické odzkoušení všech deklarovaných funkcí.

9.2 Freeware pro zálohování dat

V poslední kapitole diplomové práce se budu věnovat alternativním možnostem řešení problematiky zálohování dat z oblasti volně dostupného software čili nekomerčního freeware. Obecné označení „freeware“ pro tak důležitou úlohu jakou je zálohování dat, může ubírat na důvěryhodnosti, bezpečnosti a spolehlivosti takových aplikací. Už z tohoto důvodu, jakéhosi pocitu jistoty, když opomenu mnohdy potřebné atesty, certifikace a garance, volí každý IT profesionál komerční, osvědčený, důvěryhodný, řádně otestovaný a spolehlivý zálohovací software.

V předchozí kapitole jsem zmínil *Symantec Backup Exec* a nebylo to náhodou. S touto aplikací mám již letité a dobré praktické zkušenosti. V dřívějších letech bývala distribuována pod názvem *Veritas Backup Exec*. Aplikaci nelze upřít vysokou míru komfortu a spolehlivosti, proto ji mohu k řešení bezpečného zálohování dat ve firmách zcela jistě doporučit.

Snad každý IT profesionál vlastní své soukromé PC s daty, o které by nerad přišel. I v této profesi často platí přísloví o kovářově kobyle, většinou však do první fatální havárie pevného disku. Nastalá situace ztráty dat v konečné fázi smíření vyvolá reakci na tuto nepříjemnou skutečnost. Touto reakcí bude nepochybně hledání vhodného a levného řešení pro zálohování vlastních cenných dat. Z těží bude někdo uvažovat o robustním a na domácí poměry drahým řešením v podobě *Symantec Backup Exec*. Když opomenu další komerční zálohovací nástroje, které se běžně nabízí pro domácí uživání za relativně přijatelné ceny (např. *Acronis True Image* a jiné), pak lze vybírat z poměrně široké škály volně dostupného freeware. Jak si vybrat správně v tom nepřeberném množství různě přívětivých, avšak ne vždy zcela spolehlivých aplikací? Slušný freeware musíme trpělivě hledat a dlouho prakticky testovat, než jej nasadíme do ostrého provozu na svá cenná data.

Dobrou alternativou pro domácí potřeby datových záloh nebo pro menší počítačové sítě může být léty ověřený, spolehlivý a bezpečný zálohovací software *Cobian Backup*. Aktuální verze *Cobian Backup 10* má již plnou podporu operačního systému *Windows 7*. Umožňuje zálohovat data lokálně, ale stejně tak i po síti. Program má vestavěnou podporu šifrování zálohovaných dat *Classic PKZip*, *AES 128 - 256 bit, RSA 256 -1024 bit* (nechybí nativní generátor klíčů), *DES 64 bit* a *Blowfish 128 bit*. Umožňuje výběr ze dvou kompresních metod *ZIP* a *7Zip* včetně voleb kompresních poměrů. Umožňuje vytvářet zálohy ze stínové kopie svazku, mirroring, plánování úloh, disponuje funkcemi pro přenos archivovaných dat protokolem *FTP* na vzdálená úložiště, umožňuje vypínání a zapínání vybraných služeb, skriptů či programů před a po zálohování. Nechybí možnost nastavení odesílání logů na definované emaily. Za velkou výhodu považuji podporu dálkového ovládání distribuovaných klientů *Cobian Backup* na počítačích v síti. Mimo jiné dokáže automaticky generovat skripty pro tiché a bezobslužné instalace vzdálených klientů a poté je spravovat konzolou pro dálkové ovládání. Při instalaci programu je možné zvolit spouštění jádra *Cobian Backup* jako rezidentní služby nebo jako programové aplikace konkrétního přihlášeného uživatele. Spouštění zálohovacích úloh je také možné provádět z příkazové řádky s patřičnými parametry uvedenými v nápovědě programu.

Software je dostupný na Internetu *(www.cobiansoft.com)* a již přes 10 let ho velmi zdařile vyvíjí Luis Cobian (Švédsko). V rámci testování poslední betaverze a studie všech funkcí programu jsem pro finální verzi *Cobian Backup 10* vytvořil kompletní českou lokalizaci. Tento program je k dispozici v aktuální verzi 10.0.3.740 na přiloženém CD, které je součástí diplomové práce.

ZÁVĚR

Cílem diplomové práce je nalézt řešení pro softwarový a hardwarový audit, správu počítačů a uživatelskou podporu v podnikové síti na platformě Microsoft Windows. V současné době je k dispozici široká paleta produktů vhodných pro tyto účely. Není však možné objektivně určit jednoznačná a obecně nejvhodnější řešení. Vždy je třeba respektovat specifické individuální potřeby uživatelů konkrétní spravované domény a požadavky manažerů. Nemalou roli pak hrají finanční prostředky, čili investice do této oblasti IT. Zde je zpravidla nutné pro zadané požadavky a možnosti konkrétních řešení najít oboustranně přijatelný kompromis. Tytéž principy lze pak uplatnit i na problematiku datové bezpečnosti, která se netýká jen zálohování a archivací dat, ale také jejich zabezpečení proti neoprávněnému zneužití nebo úniku. Výsledkem diplomové práce je také analýza České legislativy platné v roce 2010 pro možnost legálního nasazení softwaru k procesu sledování činnosti zaměstnanců na svěřených počítačích.

Dílčím výsledkem může být vodítko a inspirace začínajícím správcům podnikových sítí, jak lépe systematizovat práci vlastní i samotných uživatelů. Masívní expanze nových síťových komunikačních technologií, zvláště pak webových platforem veřejné správy, prorůstajících do každodenní administrativy většiny z nás, stále více prohlubuje naši závislost na výpočetní technice. Jsem přesvědčen, že hlavní perspektivou zvyšování počítačové gramotnosti, efektivity a komfortu v užívání výpočetních technologií obecně na všech uživatelských úrovních je filozofie pozitivní motivace, kooperace a vstřícná komunikace zúčastněných stran. Iniciátor takového pokroku by měl vždy zajistit dostupnost a srozumitelnost elementárních informací, soustavné vzdělávání, flexibilní a trvalou technickou podporu stávající i nově začleňované populaci uživatelů.

ZÁVĚR V ANGLIČTINĚ

The thesis aims is to find solutions for software and hardware audit, desktop management and user support in a corporate network in Microsoft Windows platform.Currently is available wide range of products suitable for these purposes. Basicly it´s not possible to objectively determine the unique and the best solutions for general use cases. Always is necessary to respect the specific needs of individual concrete and problematic domain. Considerable role is played by the funds or investments in the IT field. There is usually necessary for the stated reguirements and the posibility of practical solutions to find a mutally acceptable compromise. The same principles can be than applied to issues of data security that is not just to be concerned only backing up and archiving data but also their security against misuse or unauthorized release. The thesis result is also Czech legislation analyze in force in 2010 for possibility of legal use to the process of monitoring the employee computer activities.

Partial result may also be a quide and inspiration for administrator beginners how better systematize their work and work of users. Massive expansion of new network communication technologies especially web public administration platform daily grows to everyday administration the most of us increasingly deeping our dependence on computer technology. I believe that the main prospect of increasing computer literacy comfort and efficiency in the use of computer technology in general at all levels of users is the philosophy of positive motivation, cooperation and friendly communication parties. Initiator of such progress should always ensure the availability and clarity of elementary information continuing education, flexible and sustained technical support to existing and newly integrating population of users.

SEZNAM POUŽITÝCH ZKRATEK

7-Zip	*7-Zip* je svobodný software vyvíjený Igorem Pavlovem a distribuovaný pod licencí GNU/GPL. Je konkurencí k známým programům jako WinZip a WinRAR.
ADIS	Automatizovaný daňový informační systém.
AES	*Advanced Encryption Standard* - Schválený standard, amerického úřadu pro standardizaci (NIST), který byl udělen symetrické blokové šifře Rijndael.
AIX	*Advanced Interactive Executive* - Název operačního systému unixového typu vyvíjeného firmou IBM.
API	*Application Program Interface* -Specifikace funkčních volání (vstupních a výstupních parametrů) programových rozhraní.
BIOS	*Basic Input-Output System* - Základní vstupně–výstupní funkce pro počítače platformy IBM PC. Představuje základní programovou výbavu pro obsluhu hardware po zapnutí počítače. Jedná se o firmware základní desky.
BMP	*Microsoft Windows Bitmap* - Počítačový formát pro ukládaní rastrové grafiky, zpravidla bez užití komprese dat.
CPU	*Central Processing Unit* - Obecné označení základní součástí počítače - procesoru.
DAS	*Data Acquisition System* - Systém integrace dat z technologických procesů do informačních systémů, a dále pak jejich vzájemná výměna mezi jinými informačními systémy.
DCOM	*Distributed Component Object Model* - Proprietární technologie pro softwarové komponenty distribuované na několik počítačů v síti pro vzájemnou komunikaci.
DES	*Data Encryption Standard* - Symetrická šifra vyvinutá v 70. letech 20. stol. V současnosti je tato šifra považována za nespolehlivou, protože používá klíč pouze o délce 64 bitů.
DFS	*Distributed File systém* - Slouží ke správě oborů názvů distribuovaného systému souborů.
DHCP	*Dynamic Host Configuration Protocol* - Aplikační protokol pro automatické přidělování IP adres počítačům v síti. Pracuje na protokolu UDP a portech 67 (server) a 68 (klient).
DNS	*Domain Name System* - Hierarchický systém doménových jmen, který převádí IP adresy na doménové jména a naopak.

EPS *Elektronický protipožární systém* - Soustava prvků, senzorů, snímačů, hasících trysek a vyhodnocovacích jednotek s výstupy stavů a automatickým hlásičem poplachu pro potřeby elektronického protipožárního zabezpečení budov a objektů.

EZS *Elektronický zabezpečovací systém* - Soustava prvků, senzorů, snímačů a vyhodnocovacích jednotek s výstupy stavů a automatickým hlásičem poplachu pro potřeby elektronického hlídání a zabezpečení budov a objektů.

GNU/GPL *GNU General Public License* - Licence pro svobodný software, původně napsaná Richardem Stallmanem pro projekt GNU.

GUI *Graphical User Interface* - Uživatelské rozhraní, které umožňuje ovládat počítač nebo programy pomocí interaktivních grafických ovládacích prvků převážně ve formě grafických oken.

HTML *HyperText Markup Language* - Značkovací jazyk pro hypertext. Je jedním z jazyků pro vytváření stránek systému World Wide Web, který umožňuje publikaci dokumentů na Internetu.

HTTP *Hyper Text Transfer Protocol* - Nejpoužívanější protokol pro přenos hypertextových dokumentů formátu HTML. Verze HTTPS umožňuje posílat data šifrovaná a tím lépe zabezpečená. Pracuje na protokolu TCP a portu 80.

HW *Hardware* - Fyzické technické vybavení počítače a periférií.

IBM *International Business Machines Corporation* - Přední světová společnost v oboru informačních technologií.

ICF *Internet Connection Firewall* - Poskytuje základní ochranu stanicím se systémem Microsoft Windows před neoprávněným vniknutím k systémovým prostředkům chráněného počítače.

IP *Internet Protocol* - Komunikační protokol používaný pro přenos dat v počítačových sítích. Je to základní protokol Internetu.

IT *Information Technology* - Informační technologie studují vše, co se týká fungování výpočetní techniky ve všech jejich technických podobách. Název je odvozen od slova informace, jelikož počítače nepracují s ničím jiným, než s daty, čili informacemi.

JPEG *Joint Photographic Experts Group* - Standardní metoda ztrátové komprese používané pro ukládání počítačových obrázků ve fotorealistické kvalitě.

LAN *Local Area Network* - Skupina počítačů a dalších zařízení propojených na relativně malé geografické oblasti, zpravidla do vzdálenosti 100 m.

MS SQL *Microsoft Structured Query Language* -
Relační databázový systém programovaný a distribuovaný firmou Microsoft.

MSDE *Microsoft SQL Desktop Engine* - Relační databázový systém vyvinutý Microsoft.

MSI *Microsoft Windows Installer* - Soubor formátu ***msi*** tvoří instalační balíček pro systémy Microsoft Windows ve formátu Windows Installer.
Soubor se může také jmenovat jako ***mps***, který slouží pro distribuci oprav již instalovaných produktů.

MySQL Multiplatformní databázový stroj. Komunikačním nástrojem je jazyk SQL.

NAS *Network Attached Storage* - Označení pro server s diskovým polem určený jako centralizované úložiště dat.

NAT *Network Address Translation* - Překlad síťových adres, je to způsob úpravy síťového provozu přes router přepisem výchozí nebo cílové IP adresy, používá se pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou.

NDIS *Network Driver Interface Specification* - Rozhraní pro programování aplikací (API) pro HW karty síťového rozhraní vyvíjený firmou Microsoft a 3Com Corporation.

NetBIOS *Network Basic Input Output System* - Síťový protokol relační vrstvy určený ke zpřístupnění dat uložených na vzdálených počítačích. Cílem je zpřístupnění síťových zdrojů a služeb pomocí názvů.

NT *New Technology* - Přeloženo jako „nová technologie“ ze které vycházejí nástupci operačního systému Windows NT, jako např. Windows 2000/XP/2003/Vista

NTFS *New Technology File System* - Souborový systém vyvinutý společností Microsoft, která jej poprvé zavedla do svého operačního systému Windows NT.

ODBC *Open Data Base Connectivity* - Standardizované softwarové API pro přístup k databázovým systémům.

OSI *Referenční model ISO/OSI* - Vypracovaný organizací ISO jako hlavní část snahy o standardizaci počítačových sítí nazvané OSI. V roce 1984 ho přijala jako mezinárodní normu ISO 7498.

PAT *Port Address Translation* - Mapování čísel TCP/UDP portů mezi veřejnou a lokální IP adresou. Několik počítačů pak může sdílet komunikaci z jedné veřejné IP adresy na různých lokálních TCP/UDP portech.

PHP *Personal Home Page* - Skriptovací programovací jazyk, určený především pro programování dynamických webových stránek.

PNG *Portable Network Graphics* - Grafický formát určený pro bezeztrátovou kompresi rastrové grafiky. Formát PNG nepodporuje systém barev CMYK.

RAM *Random Access Memory* - Vnitřní, rychlá, dočasná paměť počítače pro zápis a čtení. Informace je uchována pouze po dobu připojení ke zdroji napájení.

RFB *Remote Frame Buffer* - Jednoduchý protokol určený pro vzdálený přístup ke grafickému uživatelskému rozhraní, nejčastěji prostřednictvím počítačové sítě.

RAID *Redundant Array of Independent Disks* – Vícenásobné diskové pole nezávislých disků, prakticky se používají tři typy - RAID 0, RAID 1 a RAID 5.

RSA *Rivest Shamir Adleman* - Asymetrická šifra užívající dva klíče (veřejný a privátní), jedná se o první kryptografický algoritmus, který je vhodný jak pro podepisování, tak šifrování dat.

RSS *Really Simple Syndication* - Poskytuje obsah celého článku, příp. jeho část, odkaz na původní článek a jiná metadata. Tyto informace jsou posílány jako XML soubor nazývaný RSS zdroj, webový zdroj, RSS stream, RSS feed nebo RSS kanál.

SAN *Storage Area Network* - Je dedikovaná datová síť (LAN, WAN), která slouží pro připojení externích zařízení k serverům (disková pole, páskové knihovny a jiná zálohovací zařízení). SAN vznikla hlavně kvůli narůstajícím potřebám na zabezpečení a konsolidaci dat.

SQL *Structured Query Language* - Standardizovaný dotazovací jazyk používaný pro práci s daty v relačních databázích.

SW *Software* - Programové vybavení počítače. Sada všech počítačových programů včetně operačního systému instalovaných v počítači.

TCP *Transmission Control Protocol* - Je jedním ze základních protokolů internetu. Použitím TCP mohou aplikace na počítačích v síti vytvořit mezi sebou spojení, přes které přenáší data. Protokol je stavový a garantuje spolehlivé doručování datových bloků mezi počítači na síti.

TIFF *Tag Image File Format* - Souborových formát pro ukládání rastrové počítačové grafiky.

UDP *User Datagram Protocol* - Je dalším ze sady protokolů užívaných v síti Internet. Na rozdíl od protokolu TCP je bezstavový a nezaručuje spolehlivé doručení přenášeného datagramu.

UNC *Uniform Naming Convention* - Jednotná jmenná konvence – Zápis cesty, obecné formy názvů souborů nebo názvu adresářů, určují jedinečnou polohu v systému souborů nebo v síti.

USB *Universal Serial Bus* - Univerzální sériová sběrnice s rychlým přenosem dat. Moderní způsob připojení periférií k počítači.

VPN *Virtual Private Network* - Technologie virtuálních tunelů k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě.
Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci uzavřené privátní, lokální a tedy důvěryhodné sítě.

Wi-Fi *Wireless Fidelity* - Značka standardu pro bezdrátovou počítačovou síť.

WMI *Windows Management Instrumentation* - Systém pro jednotné ovládání různých prvků v operačním systému Microsoft Windows. Rozličné HW a SW prvky jsou chápány jako položky databáze. Je možné je jednotným způsobem hledat, zobrazovat a měnit.

WWW *World Wide Web* - Ve volném překladu „Celosvětová pavučina“, je označení pro aplikace internetového protokolu HTTP. Je tím myšlena soustava propojených hypertextových dokumentů.

XML *Extensible Markup Language* - Značkovací jazyk, který byl vyvinut a standardizován konsorciem W3C. Umožňuje snadné vytváření konkrétních značkovacích jazyků pro různé účely a různé typy dat. Zpracování XML je podporováno řadou nástrojů.

ZIP Všeobecně rozšířený souborový formát pro kompresi a archivaci dat.

SEZNAM POUŽITÉ LITERATURY

[1] Datasys s.r.o. Pilotní projekt na FŘ v Hradci Králové 2004 : Nasazení systému Windows 2003 a Exchange 2003 v rámci sítě FINet (verze 2.0). 1. vyd. Praha: DATASYS s.r.o., 2004. 478 s., 1 CD-ROM.

[2] PRICE, Brad. Active Directory : Optimální postupy a řešení problémů. Vladimír Ludva; Jindřich Jonák; Rostislav Cibulka; Martin Sodomka; Jiří Matoušek, Petr Baláš. 1. vyd. CP Books a.s., nám. 28. dubna 48, 635 00 Brno : CP Books a.s., 2005. 381 s. ISBN 80-251-0602-0.

[3] ŠETKA, Petr. Mistrovství v Microsoft Windows Server 2003 : Ze začínajícího správce expertem. Petr Klíma, Vladimír Ludva; Libor Pácl, Petr Klíma; IMIDEA; Eva Bublová, Jiří Matoušek, Pavlína Bauerová, Petr Chládek, Petr Baláš. 1. vyd. Brno : Computer Press, 2003. 680 s., 1 CD-ROM. ISBN 80-251-0036-7.

[4] WALLACE, Kevin. Cisco VoIP: Autorizovaný výukový průvodce. Jakub Hegenbart, Karel Voráček, Hana Vykoukalová, Jiří Matoušek, Petr Klíma, Daniel Štreit, Libor Pácl, Zuzana Šindlerová, Dagmar Hajdajová, Petr Baláž. 1. vyd. Brno: Computer Press, 2009. 527 s., 1 CD-ROM. ISBN 978-80-251-2228-0.

[5] RUSSINOVICH, Mark E.; SOLOMON, David A. Vnitřní architektura Microsoft Windows. 1.vyd. Brno : Computer Press, 2007. 940 s.,ISBN: 802-5112-66-7.

[6] MÜLLER, Miroslav.; KANISOVÁ, Hana. UML srozumitelně**.** Jaromír Sveřepa, Josef Novák, Eva Bublová, Jiří Matoušek, René Kašík, Martin Sodomka, Ivo Magera, Petr Klíma, Petr Baláš. 1. vyd. Brno: Computer Press, 2004. 158 s., ISBN 80-251-0231-9.

[7] MUELLER, Paul John. Příkazový řádek Windows: pro Windows Vista, 2003, XP a 2000. Milan Zelenka, Pavel Paloncý, Tomáš Mosler, Tomáš Pfanzer, Alena Laníčková, Jiří Matoušek, René Kašík, Daniel Štreit, Martin Sodomka, Libor Pácl, Zuzana Šindlerová, Daniela Nečasová. 1. vyd. Brno: Computer Press, a.s., 2008. 656 s., ISBN 978-80-251-19617.

[8] LOCKHART, Andrew. Bezpečnost sítí na maximum: 100 tipů a opatření pro okamžité zvýšení bezpečnosti vašeho serveru a sítě. Jiří Veselský, Eva Bublová, Petr Klíma, Jiří Matoušek, Daniel Štreit, Martin Sodomka, Ivo Magera, Pavel Kynický, Miroslav Hausknecht, Petr Baláš. 1. vyd. Brno: CP Books, a.s., 2005. 276 s., ISBN 80-251-0805-8.

[9] DOSTÁLEK, Libor.; VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Luděk Rašek, Marie Schreinerová, Jiří Matoušek, Martina Petrová, Iva Vilímská, Martin Sodomka, Ivo Magera, Petr Klíma, Pavel Kynický, Zuzana Šindlerová, Petr Baláš. 1. vyd. Brno: Computer Press, a.s., 2006. 534 s., ISBN 80-251-0828-7.

[10] PUSTKA, Josef. Komunikace s počítačem mluvenou řečí. RNDr. Ivan Kramosil, DrSc., doc. Ing. Jiří Lažanský, Csc., Oleg Man, Mgr. Aleš Baďura, Antonín Bartoušek. 1. vyd. Praha: Academia, 1995. 287 s., ISBN 80-200-0203-0.

[11] KOSEK, Jiří. PHP – Tvorba interaktivních internetových aplikací. Václav Urban, Adéla Bělovská. 1. vyd. Praha: Grada Publishing, a.s., 1998. 492 s. ISBN 80-7169-373-1.

[12] IVENS, Kathy. Microsoft Exchange 5.5: Kapesní rádce administrátora. Jan Škvařil, Veronika Macková, Jiří Matoušek, Tomáš Kuchař, Jaroslav Novák, Ivo Magera, Mirek Zachrdle, Martin Hanslian, Kateřina Vobecká. 1. vyd. Praha: Computer Press 1999. 248 s. ISBN 80-7226-228-9.

[13] SCAMBRAY, Joel.; McCLURE, Stuart.; KURTZ George. Hacking bez tajemství, 2. aktualizované vydání. Petr Břechovský, Josef Pojsl, Radek Čevela, Libor Dostálek, Marie Schreinerová, Petr Klíma, Martin Hanslian, Pavlína Bauerová, Ivana Mitáčková, Ivo Magera, Mirek Zachrdle, Pavla Větříšková, Petr Baláš. 2. vyd. Praha: Computer Press 2002. 625 s., 1 CD-ROM. ISBN 80-7226-644-6.

[14] Fair Net spol. s.r.o : [online]. Text v češtině, angličtině, slovenštině. Dostupný z WWW: <http://www.fairnet.cz/>

[15] Label software s.r.o., Software: Dozorce. [online]. Text v češtině. Dostupný z WW: <http://www.dozorce.cz/>

[16] Microsoft corporation: [online]. Text v češtině, angličtině. Dostupný z WWW: <http://www.microsoft.cz/>

[17] TruconneXion a.s., Software: AuditPro. [online]. Text v češtině, angličtině, slovenštině, polštině, maďarštině, ruštině. Dostupný z WWW: <http://www.auditpro.cz/>

[18] Windows Sysinternals, Software: PSTools. [online]. Text v angličtině. Dostupný z WWW: <http://www.sysinternals.com/>

[19] Per Skjerpe, Software: WinGrab. [online]. Text v češtině. Dostupný z WWW: <http://www.slunecnice.cz/sw/wingrab//>

[20] PX Server – IT Solution, Software: WinAudit : [online]. Text v angličtině. Dostupný z WWW: <http://www.pxserver.com/>

[21] ManicTime, Software: ManicTime : [online]. Text v angličtině.Dostupný z WWW: <http://www.manictime.com/>

[22] VertrigoServ, Software: VertrigoServ: [online]. Text v angličtině. Dostupný z WWW: <http://vertrigo.sourceforge.net/>

[23] Wikipedie : [online]. Text v češtině. Dostupný z WWW: <http://cs.wikipedia.org/>

[24] Informační systém ALVAO Asset Management : [online]. Text v češtině. Dostupný z WWW: <http://www.alc.cz/>

[25] eDetektiv, Software: eDetektiv : [online]. Text v češtině. Dostupný z WWW: <http://www.edetektiv.cz/>

[26] Sparx Systems, Software: Enterprise Architect 7.5: [online]. Text v angličtině. Dostupný z WWW: <http://www.sparxsystems.com/>

[27] Symantec, Data Protection, Software: Symantec Backup Exec: [online]. Text v angličtině. Dostupný z WWW: <http://www.symantec.com/business/solutions/>

SEZNAM OBRÁZKŮ

Obrázek 1: Referenční model OSI [23].....12
Obrázek 2: Síťová architektura Windows [5].....13
Obrázek 3: Implementace podnikového informačního portálu.....23
Obrázek 4: Servisní kniha pro podporu uživatelů.....23
Obrázek 5: Informace o postupu a stavu řešeného požadavku.....24
Obrázek 6: Správa počítače z Active Directory.....26
Obrázek 7: Vztahy mezi komponentami PCInfoMagicEYE.....31
Obrázek 8: Ukázka výstupu auditu PCInfo za celou organizaci.....33
Obrázek 9: Správa vzdálené stanice z PCInfo desktop 34
Obrázek 10: Nastavení aplikace PCInfo MagicEYE Desktop.....47
Obrázek 11: Nastavení položek dialogového okna PCInfo auditu.....48
Obrázek 12: Nastavení hloubky auditu.....49
Obrázek 13: Okno přihlášení k programu Dozorce.....52
Obrázek 14: Modul RemRun pro vzdálenou instalaci Dozorce.....52
Obrázek 15: Skryté umístění programu Dozorce ve složce Windows 52
Obrázek 16: Klíč v registrech pro spuštění Dozorce po startu Windows.....53
Obrázek 17: Nastavení odesílání dat v programu Dozorce.....54
Obrázek 18: Záznam tabulky událostí v programu Dozorce 54
Obrázek 19: Graf aktivity uživatele v čase dle užití klávesnice a myši.....55
Obrázek 20: Graf aktivních a užitých programů během pracovní doby.....55
Obrázek 21: Graf vytížení procesoru (počítače).....55
Obrázek 22: Graf vytížení operační paměti RAM.....56
Obrázek 23: Využití kapacity připojených logických diskových jednotek.....56
Obrázek 24: Část tabulky se souhrnnými údaji monitoringu Dozorce.....56
Obrázek 25: Možnosti nastavení v programu ManicTime.....59
Obrázek 26: Zobrazení aktivit na časových osách ManicTime.....59
Obrázek 27: Navštívené webové stránky a doba prohlížení.....60
Obrázek 28: Týdenní graf činnosti a nečinnosti počítače 60
Obrázek 29: Nefunkční Microsoft Exchange server 63
Obrázek 30: Změna platného telefonu HOT-LINE v době nepřítomnosti.....63
Obrázek 31: Okno nápovědy MSI.....66
Obrázek 32: Vzdálené operace se soubory a složkami uživatelů 68

SEZNAM PŘÍLOH

PŘÍLOHA I.: Návrh aplikace technické podpory uživatelů 87
PŘÍLOHA II. : Protokoly SW a HW auditu.....92
PŘÍLOHA III. : Audit programem WinAudit.....100
PŘÍLOHA IV. : Monitorovací systém Dozorce.....108
PŘÍLOHA V. : Kód pro odinstalaci klienta PCInfo MagicEYE.....115

PŘÍLOHA I.: Návrh aplikace technické podpory uživatelů

SERVICE BOOK - Requirements

R001: Zobrazení seznamu servisních požadavků

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

První strana servisní knihy udržuje přehledný a kontinuální seznam servisních požadavků. Obsahuje tyto objekty: **Předmět požadavku, Jméno a příjmení uživatele, Datum a čas zadání, Odkaz na detail požadavku.** Seznam požadavků se bude stránkovat po 10 zobrazených předmětech v seznamu. Číselné odkazy pro listování mezi stránkami seznamu požadavků budou umístěny pod seznamem požadavků a budou řazeny vzestupně.

R002: Ošetření vyjímek

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Okno vyjímky ze zobrazí, pokud nebudou vyplněny povinné položky formulářů *(Jméno a příjmení uživatele, Jméno a příjmení řešitele, Předmět požadavku, Popis požadavku, Vyjádření řešitele, ID heslo, Bezpečnostní heslo)* tzn. budou mít nulovou hodnotu či prázdné pole.

Okno vyjímky zobrazí tento text: **Nejsou vyplněny všechny povinné požadované položky.** Dále pak bude mít URL odkaz na: **Návrat na předcházející formulář.**

R003: Zobrazení diagnostických návěští

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Systém bude automaticky po načtení úvodní stránky servisní knihy zobrazovat informační diagnostický panel – pruh, s barevnými návěštími o stavu provozu vybraných služeb. Zobrazované informace na panelu budou návratové hodnoty diagnostických funkcí pro kontrolu stavu ON-LINE či OFF-LINE vybraných sdílených služeb. Jsou jimi tyto služby: **IS ADIS, Proxy, Exchange, Docházka.**

R004: Odběr avíz RSS kanálem

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Pata všech stránek bude obsahovat URL odkaz pro odběr informačních avíz přes RSS kanál. RSS funkce bude dávat možnost všem uživatelů přes libovolnou čtečku kanálů RSS odebírat avíza o aktuálních nahlášených požadavcích a stavu jejich řešení.

R005: Zobrazení detailu požadavku

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Detail požadavku je samostatná stránka - karta v prohlížeči s detailním popisem servisního požadavku. Obsahuje tyto položky: **Stav požadavku**, **Předmět požadavku, Odkaz na seznam požadavků, Jméno a příjmení uživatele, Datum a čas zadání, IP adresu, Popis požadavku.** Spodní část karty obsahuje: **Jméno a příjmení řešitele, Datum a čas odpovědi, IP adresu, Vyjádření řešitele.**

Pata stránky bude mít dostupný URL odkaz na formulář pro **Řešitel požadavku**, **Odběrový RSS kanál** a zobrazenou hodnotu **Počítadla zobrazení**.

R006: Formulář pro zadání servisního požadavku

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Úvodní strana servisní knihy bude mít pod diagnostickým panelem uživatelský formulář pro zadání servisního požadavku s těmito položkami: **Předmět požadavku, Jméno a příjmení uživatele, Popis požadavku, Tlačítko ODESLAT.** Tlačítkem ODESLAT se událost zařadí do seznamu servisních požadavků. Automaticky mu bude přiřazen stav požadavku: **NOVÝ.** Uživatel musí zadat hodnoty všech atributů formuláře, jinak bude zobrazeno **okno vyjímky.**

R007: Formulář pro vložení odpovědi řešitele

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Karta bude jako nové okno v prohlížeči po kliknutí na URL odkaz **Řešitel požadavku,** který bude dostupný pouze na kartě **Detail požadavku** a bude se vztahovat k aktuálně zobrazovanému požadavku. Zde se zadá odpověď či vyjádření řešitele na daný servisní požadavek. Řešitel může zadávat libovolný počet odpovědí na jeden požadavek uživatele v souvislosti s jeho stavem řešení. Ke každému vyjádření řešitele se zobrazí datum a čas, případně změna stavu stádia řešení.

Formulář řešitele požadavků obsahuje tyto položky: **Odkaz na seznam požadavků, ID požadavku, Předmět požadavku, Jméno a příjmení řešitele, Vyjádření řešitele, Stav požadavku, ID heslo, tlačítko ODESLAT.** Pata formuláře bude mít dostupný URL odkaz : **Editace souborů** pro případnou úpravu textů v datových souborech. Jinde nebude tento odkaz dostupný.

R008: Formulář pro editaci datových souborů

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Formulář pro přímou editaci textů uložených v datových souborech se otevře v nové záložce prohlížeče po kliknutí na URL odkaz **Editace souborů.** Ten bude dostupný pouze na formuláři řešitele požadavků. Slouží ke zpětné korekci, doplnění, úpravě a případnému mazání textů uložených v datových souborech.

Obsahuje tyto položky: **Editace předmětu požadavku, Editace popisu požadavku, Editace jména a příjmení uživatele, Editace jména a příjmení řešitele, Editace vyjádření řešitele, Editace stav požadavku, Bezpečnostní heslo.** Každá položka se může editovat zvlášť ve svém poli a má vlastní tlačítko **ULOŽIT** pro uložení opraveného textu. Uložení opravy vyžaduje zadání bezpečnostního hesla.

R009: Seznam uživatelů

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Každý uživatel je zavedený v databázi zaměstnanců. Při zadávání servisního požadavku se z tohoto seznamu vybere jako zadavatel požadavku. Pokud nebude vybrána položka zadavatele požadavku, bude zobrazeno okno vyjímky. Položkami ve výběrovém seznamu uživatelů je: **Jméno, Příjmení.**

R010: Seznam řešitelů

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Každý řešitel je zavedený v databázi oprávněných řešitelů. Při zadávání vyjádření řešitele si z tohoto seznamu řešitel vybere své jméno. Před uložením odpovědi na požadavek musí zadat své ID heslo, jinak bude zobrazeno okno vyjímky. Položkami ve výběvém seznamu jsou: **Jméno a příjmení řešitele, ID heslo.**

R011: Aktuální stav požadavku

«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Stav požadavku **NOVÝ** se automaticky vygeneruje při odeslaní nového servisního požadavku. Změnit ho lze pouze na kartě **Řešitel požadavku** před odesláním odpovědi řešitele, kde je výběrovou položkou formuláře **Stav požadavku** s těmito volbami: **Nový, Rozpracovaný, Čekající, Postoupený, Odložený, Neřešený, Ukončený.**

Implicitně je zobrazován aktuální stav požadavku.

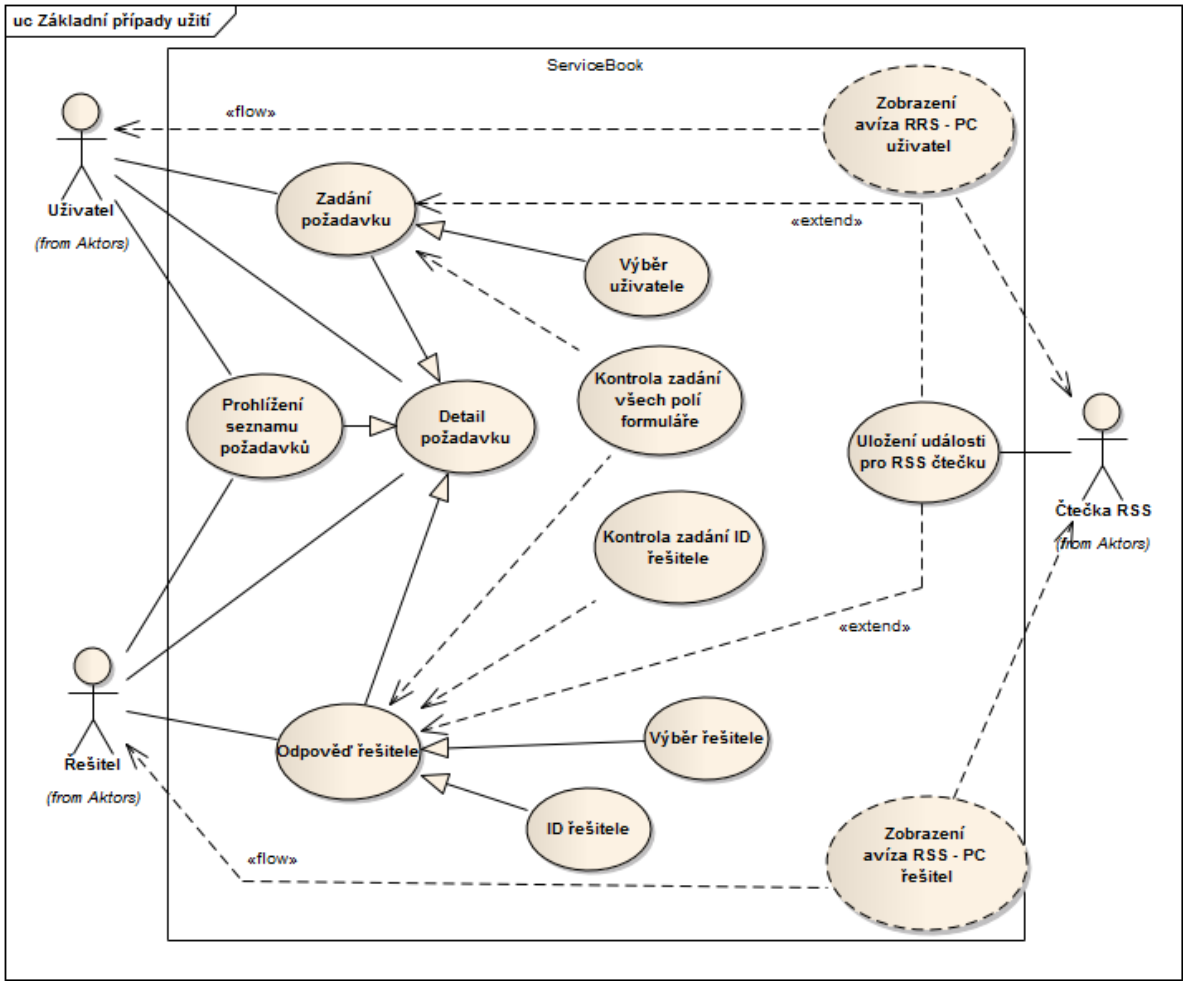
R012: Počítadlo zobrazení detailu požadavku

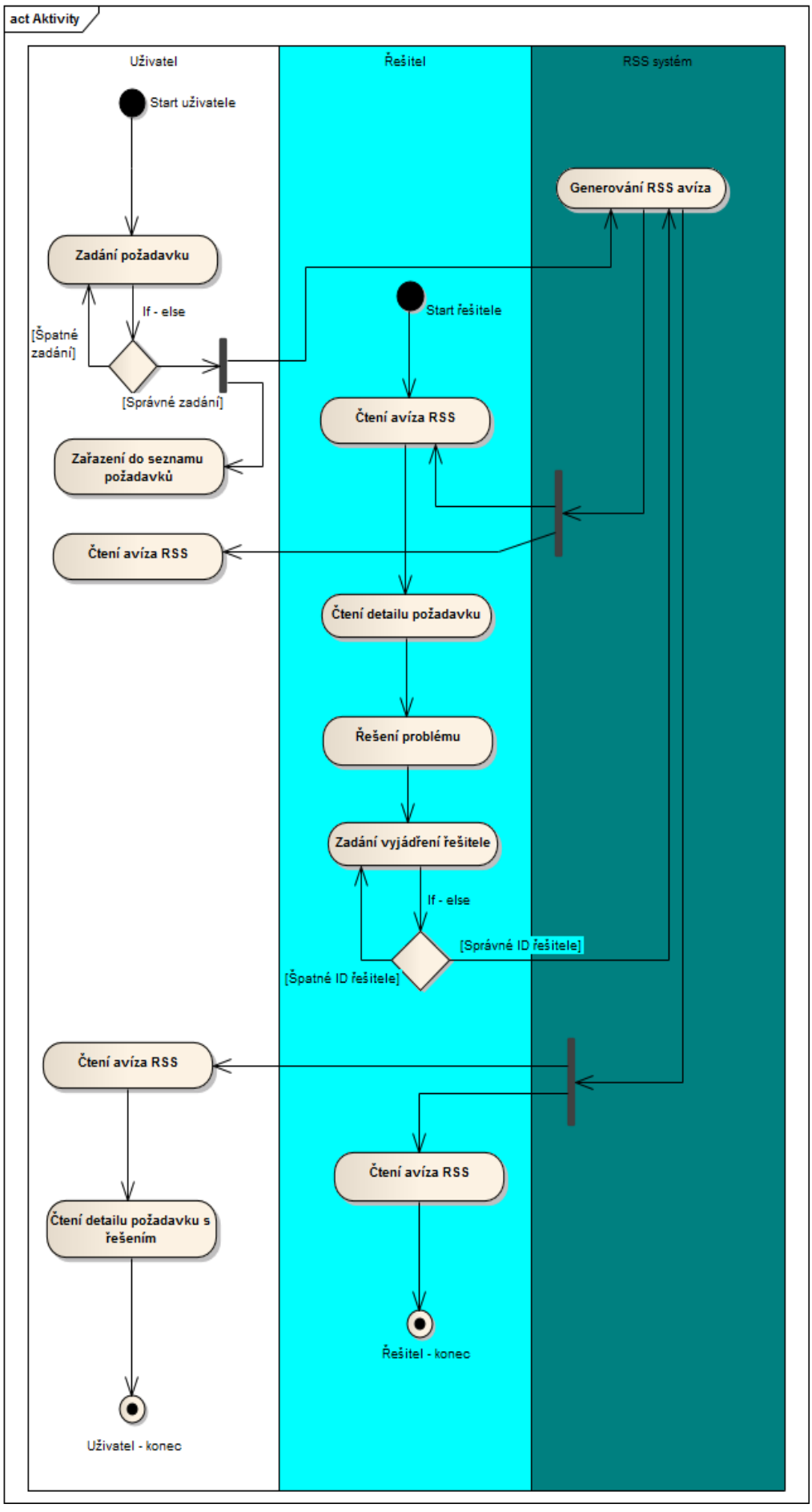
«Functional» *Satus:* *Priority:* *Difficulty:* Medium

Proposed Medium

Phase: 1.0 *Version: 1.0*

Počítadlo bude zobrazovat aktuální číselnou hodnotu celkového počtu zobrazení stránky s detailem servisního požadavku. Počítadlo bude umístěno pouze na kartě detailu požadavku. V jeho patičce.




act Aktivity
Uživatel
Řešitel
RSS systém
Start uživatele
Generování RSS avíza
Zadání požadavku
If - else
[Špatné zadání]
[Správné zadání]
Start řešitele
Čtení avíza RSS
Zařazení do seznamu požadavků
Čtení avíza RSS
Čtení detailu požadavku
Řešení problému
Zadání vyjádření řešitele
If - else
[Správné ID řešitele]
[Špatné ID řešitele]
Čtení avíza RSS
Čtení avíza RSS
Čtení detailu požadavku s řešením
Řešitel - konec
Uživatel - konec

PŘÍLOHA II. : Protokoly SW a HW auditu

Předávací protokol počítače:

Předávací protokol počítače Strana: 1

pro Finanční úřad v Moravské Třebové 10.2.2010

Název serveru

Identifikace počítače

Jméno počítače:	Název serveru	**Příjmení a jméno:**	FUMOTNT2
Název počítače:		**Číslo kanceláře:**	309
PCinfo id:	4f6296fa	**Inventární číslo PC:**	43924
Jméno disku C:		:	
IP adresa:	xxx.xxx.xxx.xxx	:	
MAC adresa:	xx-xx-xx-xx-xx-xx	:	
E-mail:		:	
Spec. id. - popis:		:	
Spec. id. - hodn.:		:	
Název id. pole0:	265-FÚ v Moravské Třebové:		
Hodnota id. pole0:	970-daňová správa		
Windows prod. klíč:	xxxxx-xxxxx-xxxxx-xxxxx-xxxxx		

Uživatel

Jméno: Zukal Jiří **Telefon:** +420 461 xxx xxx **Mobil:** +420 728xxxxxx

Email: Jiri.Zukal@mot.hk.ds.mfcr.cz

Organizační jednotka

Organizační jednotka: 970-daňová správa

Lokalita

Lokalita:

Hardwarová konfigurace počítače

Počítač:	AT/AT COMPATIBLE
Procesor:	Intel, Pentium 4, 0F29h, 2660MHz
Paměť:	2048MB, 2, 767MB
Disk1:	IC35L060AVV207-0, IDE, 40.02GB, VNVB30G2UAA0JV
Disk2:	LSI, LSI MegaIDE #00, SCSI, 80.02GB
Disketa1:	3.5 1.44, A
CD-ROM1:	CD-ROM GCR-8482B/HL-DT-ST, CD-ROM GCR-8482B/HL-DT-ST
Grafická karta:	RAGE, RAGE XL PCI Family (Microsoft Corporation)
Zvuková karta:	Realtek AC 97 Audio
Síťová karta:	Broadcom, Broadcom NetXtreme Gigabit Ethernet, Broadcom NetXtreme Gigabit Ethernet, b57w2k, 0C
Monitor:	IQT1773
Klávesnice:	Standard 101/102-Key or Microsoft Natural PS/2 Keyboard
Myš:	PS/2 Compatible Mouse

Softwarová konfigurace počítače

Jméno výrobce	Jméno programu	Verze	Nalezen	Počet
Adobe	Acrobat Reader32		☑ Y	1
Microsoft Corporation	Exchange Server 2003		☑ Y	2
Adobe	Installation Acrobat Reader32 EN	4.05	☑ Y	1
Archivers	LHARC		☑ Y	1
Microsoft Corporation	Microsoft .NET Framework	1.1.4322.57	☑ Y	1
Microsoft Corporation	Microsoft .NET Framework	3.0.4506.64	☑ Y	1
Microsoft Corporation	Microsoft® .NET Framework	2.0.50727.4	☑ Y	1

Předávací protokol počítače
pro Finanční úřad v Moravské Třebové

Strana: 2
10.2.2010
[redacted]

IBM Corporation	PC DOS	6.0	☑ Y	1
FairNet, spol. s r.o.	PCinfo Client	7.5	☑ Y	1
Microsoft Corporation	SQL Server	8.00.194	☑ Y	1
Microsoft Corporation	SQL Server	8.00.760	☑ Y	1
Symantec Corporation	Symantec AntiVirus	9.0.2.1000	☑ Y	1
Microsoft Corporation	Windows 2003 Server		☑ Y	1
Microsoft Corporation	Windows Media Player	10.0	☑ Y	1
Microsoft Corporation	Windows NT EN	4.0	☑ Y	1

Ostatní přiřazený majetek

Typ majetku	Jméno majetku	Evidenční číslo	Inventární číslo	Výrobní číslo

Údaje o OS

Jméno OS: Microsoft(R) Windows(R) Server 2003,
Verze: 5.2.3790
Číslo SP: 2
Registrovaná společnost: FINet
Registrovaný uživatel: FU v Moravske Trebove
Windows digital id: xxxxx-xxx-3051212-45320
Windows produktový kód: [redacted]
Office produktový kód:

MSI informace

Jméno programu	Verze	Společnost	Uživatel	Sériové číslo
Adobe Reader 9.2 - Czech	9.2.0	FINet	FU v Moravske	none
IIS 6.0 Resource Kit Tools	6.00.0000			
Microsoft .NET Framework	1.1.4322	FINet	FU v Moravske	56056-463-2045012-04326
Microsoft .NET Framework	2.1.21022			
Microsoft .NET Framework	3.1.21022	FINet	FU v Moravske	none
Microsoft Application Error	11.0.5228.1			
Microsoft Application Error	11.0.5614.0			
Microsoft Windows Czech	1.0.705.0			
Microsoft XML Parser	8.50.2162.6	FINet	FU v Moravske	none
MSXML 4.0 SP2 (KB927978)	4.20.9841.0	FINet	FU v Moravske	none
MSXML 6.0 Parser	6.10.1200.0	FINet	FU v Moravske	none
Security Update for	2.1.0.2	FINet	FU v Moravske	none
Symantec AntiVirus	9.0.210			
Symantec Backup Exec	11.0.7170			
Symantec Mail Security 4.6	4.6			
Symantec Mail Security for	4.6			
Windows Presentation	3.0.6920.0	FINet	FU v Moravske	none
Windows Resource Kit Tools	5.2.3790	FINet	FU v Moravske	12345-111-1111111-04692

Předávací protokol počítače

pro Finanční úřad v Moravské Třebové

Strana: 3
10.2.2010
Název serveru

Windows Support Tools	5.2.3790	FINet	FU v Moravske	12345-111-1111111-21878

Dne:	.....	Dne:	.....	Dne:	.....
Předal(a):	.....	Převzal(a):	.....	Schválil(a):	.....
Podpis:	.....	Podpis:	.....	Podpis:	.....

Zde si můžete vložit Vaši poznámku

Celkový počet stran: 3

* * * Konec sestavy * * *

Specifikační list počítače:

Specifikační list počítače Strana: 1

pro Finanční úřad v Moravské Třebové 10.2.2010

Název PC

Identifikace počítače

Jméno počítače:	Název PC	**Příjmení a jméno:**	Zukal Jiří
Název počítače:		**Číslo kanceláře:**	310
PCinfo id:	6f697acd	**Inventární číslo PC:**	52718
Jméno disku C:	system	:	
IP adresa:	xxx.xxx.xxx.xxx	:	
MAC adresa:	xx-xx-xx-xx-xx-xx	:	
E-mail:		:	
Spec. id. - popis:		:	
Spec. id. - hodn.:		:	
Název id. pole0:	265-FÚ v Moravské Třebové:		
Hodnota id. pole0:	970-daňová správa		
Windows prod. klíč:			

Uživatel

Jméno: Zukal Jiří **Telefon:** +420 461 xxx xxx **Mobil:** +420 728xxxxxx

Email: Jiri.Zukal@mot.hk.ds.mfcr.cz

Organizační jednotka

Organizační jednotka: 970-daňová správa

Lokalita

Lokalita:

Hardwarová konfigurace počítače nebyla auditována

Softwarová konfigurace počítače

Jméno výrobce	Jméno programu	Verze	Nalezen	Počet

Údaje o OS

Jméno OS:	**Verze:**	**Číslo SP:**
Microsoft Windows XP Professional	5.1.2600	3
Registrovaná společnost:	**Registrovaný uživatel:**	**Windows digital id:**
Finanční ředitelství Hradec Králové	Finanční úřad v Moravské Třebové	xxxxx-xxx-1435852-23501
Windows produktový kód:	**Office produktový kód:**	
	xxxxx-xxxxx-xxxxx-GJFMT-3GYQY	

MSI informace

Jméno programu	Verze	Společnost	Uživatel	Sériové číslo
Adobe Reader 9.3 - Czech	9.3.0	Finanční ředitelství	Finanční úřad v	none
Broadcom Management	9.03.02	Finanční ředitelství	Finanční úřad v	none
Broadcom NetXtreme	9.02.06	Finanční ředitelství	Finanční úřad v	none
HP Precisionscan Pro 3.1	3.1.0.0000	Finanční ředitelství	Finanční úřad v	None
Microsoft .NET Framework	2.1.21022			
Microsoft .NET Framework	2.1.21022			
Microsoft .NET Framework	3.1.21022	Finanční ředitelství	Finanční úřad v	none
Microsoft .NET Framework	3.1.21022	Finanční ředitelství	Finanční úřad v	none
Microsoft .NET Framework 3.5	3.5.21022			

Specifikační list počítače Strana: 2

pro Finanční úřad v Moravské Třebové 10.2.2010

Název PC

Microsoft .NET Framework	3.5.21022			
Microsoft Office 2000 SR-1	9.00.9327	Finanční ředitelství	Finanční úřad v	51255-270-4715693-02075
Microsoft Office Outlook 2003	11.0.5614.0	Finanční ředitelství	Finanční úřad v	74478-640-1246787-55235
Security Update for	2.1.0.2	Finanční ředitelství	Finanční úřad v	none
Symantec AntiVirus	10.1.5000.5			
WebFldrs XP	9.50.7523	Finanční ředitelství	Finanční úřad v	12345-111-1111111-18228

Dne:	.....	Dne:	.....	Dne:	.....
Předal(a):	.....	Převzal(a):	.....	Schválil(a):	.....
Podpis:	.....	Podpis:	.....	Podpis:	.....

Zde si můžete vložit Vaši poznámku

Celkový počet stran: 2

* * * Konec sestavy * * *

Nalezené programy

Strana: 1

pro Finanční úřad v Moravské Třebové

10.2.2010

Jméno výrobce / Jméno programu	Popis / Verze	Zakoupeno	Nalezeno	Rozdíl
Adobe				
Acrobat Reader32			30	-30
Installation Acrobat Reader32 EN	4.05		1	-1
Microsoft Corp. - Office				
Access 2000 OEM/Installation			1	-1
Excel 2000			27	-27
Excel 2000 OEM/Installation			1	-1
FrontPage 2000 OEM/Installation			1	-1
Outlook 2000 OEM/Installation			1	-1
PowerPoint 2000			27	-27
PowerPoint 2000 OEM/Installation			1	-1
Word 2000			27	-27
Word 2000 OEM/Installation			1	-1
Outlook 2003		28	27	1
Symantec Corporation				
Symantec AntiVirus	10.1.5.5000		21	-21
Symantec AntiVirus	10.1.5.5010		1	-1
Symantec AntiVirus	9.0.2.1000		4	-4
Microsoft Corporation				
Exchange Server 2003			4	-4
Microsoft .NET Framework	1.1.4322.573		21	-21
Microsoft .NET Framework	3.0.4506.30		7	-7
Microsoft .NET Framework	3.0.4506.648		16	-16
Microsoft .NET Framework	3.5.21022.8		5	-5
Microsoft Script Debugger	1.00.7295		1	-1
Microsoft SQL Server 2005			2	-2
Microsoft SQL Server 2005	9.00.2047.00		1	-1
Microsoft Windows Server Update Services	3.0		1	-1
Microsoft® .NET Framework	2.0.50727.42		31	-31
PowerPoint Viewer	97		28	-28
Snapshot Viewer	9.0.0.2602		1	-1
SQL Server	7.00.623		1	-1
SQL Server	8.00.194		1	-1
SQL Server	8.00.760		2	-2
Windows 2000			1	-1
Windows 2003 Server			4	-4
Windows Media Encoder	9.x		1	-1
Windows Media Player	10.0		3	-3
Windows Media Player	11.0		6	-6
Windows Media Player	9.0		33	-33
Windows NT EN	4.0		1	-1

Nalezené programy – souhrnná sestava za celou organizaci:

Nalezené programy Strana: 2

pro Finanční úřad v Moravské Třebové 10.2.2010

Jméno výrobce / Jméno programu	Popis / Verze	Zakoupeno	Nalezeno	Rozdíl
Windows XP CZ	5.1.2600.0		38	-38
FairNet Distribution, spol. s r.o.				
PCinfo Client	5.0		1	-1
PCinfo Desktop	4.0.1.2		1	-1
Christian Ghisler				
Total Commander	6.53		1	-1
CyberLink Corp.				
CyberLink PowerDVD	7.0.0.1024		5	-5
PowerDVD DX	8.02		8	-8
Freeware				
LAME			1	-1
PDFCreator	0.09.0005		1	-1
Přečíslování			1	-1
IBM Corporation				
PC DOS	6.0		2	-2
Citrix Systems				
Citrix ICA Client	10.0		1	-1
Citrix ICA Client	9.00		4	-4
ATI Technologies Inc.				
Catalyst Control Centre	1.2		2	-2
Alis s.r.o.				
UFAND			1	-1
Archivers				
LHARC			1	-1
PowerArchiver CZ	6.00		8	-8
RAR			1	-1
CaseWare International Inc.				
IDEA	7.3		3	-3
Entrust Technologies				
Entrust Solo			1	-1
FBL Group				
ArcTel 32	4.21		2	-2
ArcTel 32	4.24		46	-46
Inprise Corporation (Borland)				
Borland DB engine			3	-3
Irfan Skiljan				
IrfanView	3.75		5	-5
MySQL AB				
MySQL			1	-1
Software602				

Nalezené programy Strana: 3

pro Finanční úřad v Moravské Třebové 10.2.2010

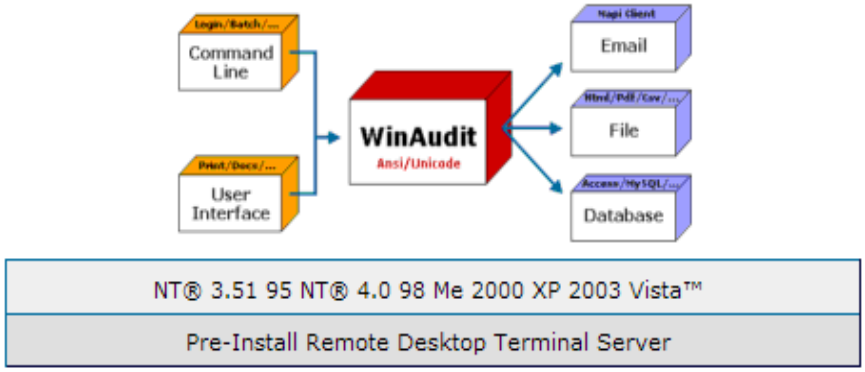
Jméno výrobce / Jméno programu	Popis	Verze	Zakoupeno	Nalezeno	Rozdíl
602XML Filler		2.5.6		1	-1
Sun Microsystems Inc.					
Java Runtime Environment SE		1.4.x		14	-14
Java Runtime Environment SE		1.5.x		12	-12
Java Runtime Environment SE		1.6.x		13	-13
The PHP Group					
PHP				1	-1
Utilities					
PrintKey 2000		5.1.0.0		1	-1
FairNet, spol. s r.o.					
MagicMONITOR Agent		7.5		2	-2
PCinfo Client	swinfo32	7.5		34	-34
PCinfo Desktop	PCinfo Desktop	7.5		2	-2
ASPI, a.s.					
ASPI Client				1	-1
Cinematronics					
Pinball 3D				21	-21

Celkový počet stran: 3

* * * Konec sestavy * * *

PŘÍLOHA III. : Audit programem WinAudit

Schema I/O funkcí programu WinAudit:



Command line parametry programu WinAudit:

To view the command line usage, at the command prompt, type:
WinAudit.exe /h

To audit your computer showing only the System Overview and to save the report in the default TEXT format using the default filename of 'computername.txt'.
WinAudit.exe /r=g

To audit your computer showing the System Overview and Operating System sections and to save the report in TEXT format in directory C:\Temp
WinAudit.exe /r=go /f=C:\Temp

To audit your computer showing the System Overview, Operating System and Installed Software sections and to save the report in CSV format with filename 'computername.csv' on a remote computer called SERVER in the networked shared directory Audits
WinAudit.exe /r=gos /o=CSV f=\\SERVER\Audits

To save the audit as a PDF document with the password smith.
WinAudit.exe /r=gos /o=PDF /p=smith

To send the audit to an Access database specified by the Data Source Name (DSN) 'AccessDSN' that is not password protected.
WinAudit.exe /r=gos /o=ODBC /f=AccessDSN

To send the audit to a SQL Server(TM) database specified by the Data Source Name (DSN) 'SQLServerDSN' using the user name 'John' and the password 'Smith'.
WinAudit.exe /r=gos /o=ODBC /f=SQLServerDSN /u=John /p=Smith

To scan your hard drives for executables and zip files and save the information in MyFiles.html with images. Stop if this is taking more than 5 minutes.
WinAudit.exe /r=F /f=MyFiles.html /o=HTMLi /e="exe zip" /t=5

Get a System Overview and log the audit to a file called log.txt. The audit will be saved in 'computername.txt'.
WinAudit.exe /r=g /l=log.txt

Get a System Overview with the user seeing a custom message displayed in a window. The audit will be saved in 'computername.txt'.
WinAudit.exe /r=g /m=The network administrator is examining this computer.

Get a lot of categories using Italian translation strings where possible and save the output in XML format.
WinAudit.exe /r=gsoPxuTUeNt /o=XML /L=it

Get some data in html format and save the output using the MAC address as the file name. This enables data for machines that have the same name to be saved in the same directory. Image file names specific to the computer, such as memory usage, will be prepended with the MAC address.
WinAudit.exe /r=gsmd /o=HTMLi /f=%LOGONSERVER%\temp\macaddress

Get a report of the software on the computer and save it in compiled html format. The output will be saved to 'computername.chm'. For this to work the computer must have Html Help Workshop installed.
WinAudit.exe /r=s /o=chm

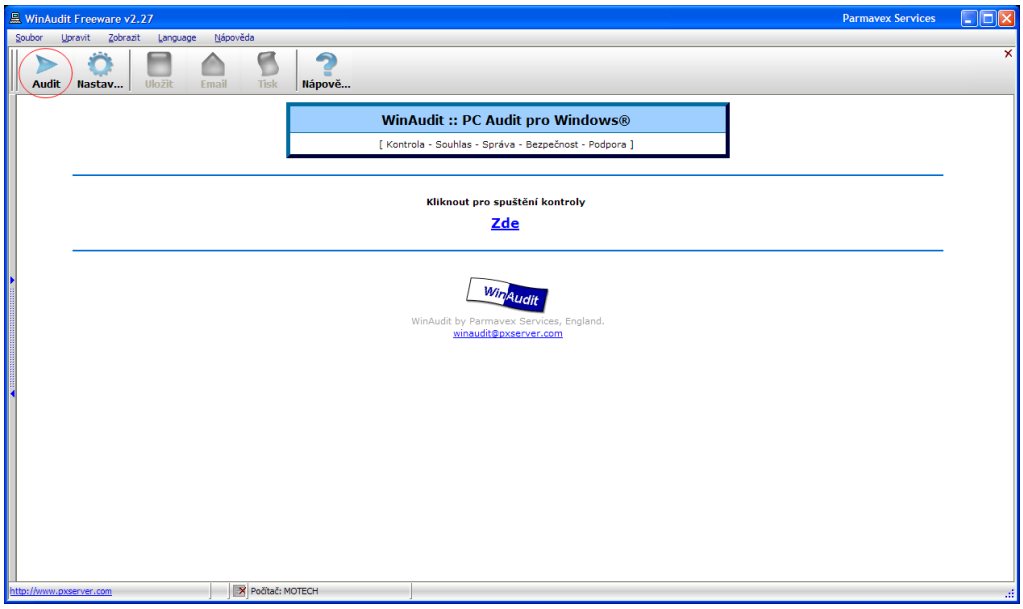
Send a system overview to a database specified by a machine independent data source (File DSN) named database.dsn. The File DSN must be in the user's default DSN directory which is specified in the registry as key *DefaultDSNDir* at HKEY_CURRENT_USER\Software\ODBC\ODBC.INI\ODBC File DSN. If this registry key does not exist, the File DSN must be in the 'ODBC\Data Sources' directory below the system level directory specified as key *CommonFilesDir* at HKEY_LOCAL_MACHINE\SOFTWARE\Micr osoft\Windows\CurrentVersion, e.g. 'C:\Program Files\Common Files\ODBC\Data Sources'.
WinAudit.exe /r=g /o=ODBC /f=database.dsn

Send a system overview to an Access database using a DSN-Less connection string. The string must have the keyword DRIVER, have no forward slashes and must not end with .dsn.
WinAudit.exe /r=g /o=ODBC /f=DBQ=C:\access.mdb;Driver={Microsoft Access Driver (*.mdb)};UID=admin;

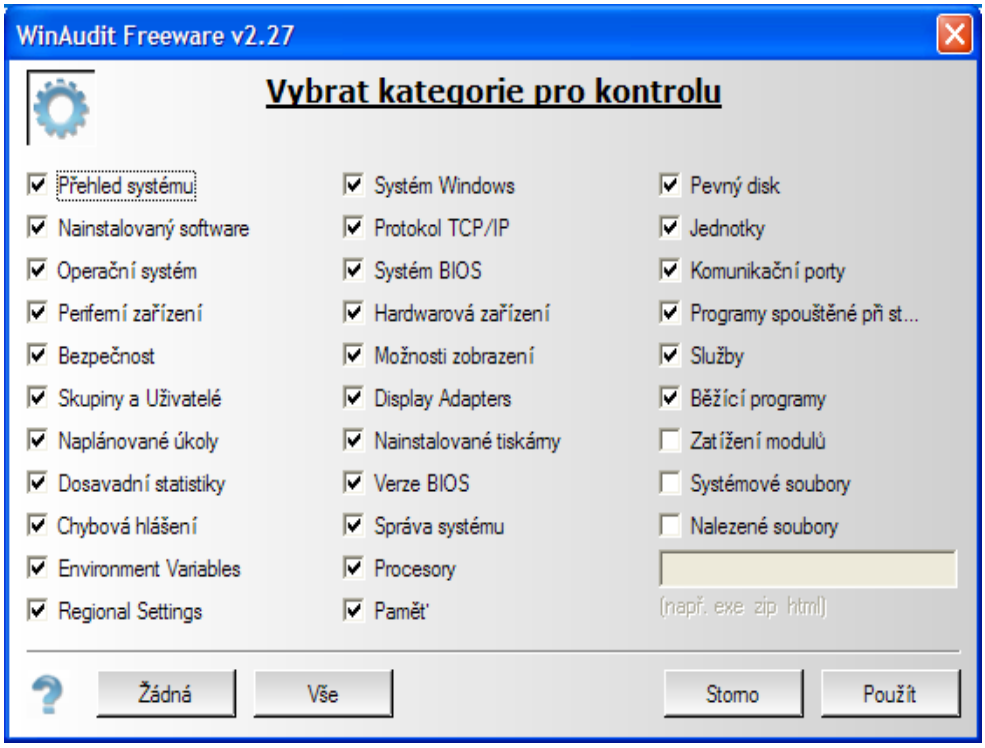
Send a system overview to SQL Server on a computer named PXSSQLSVR using a DSN-Less connection string. Connect as system administrator (sa) to a database named winauditdb and write out a log file to log.txt. On successful connect, the Completion Connection String will be reported in the log file. Note, there is a space between 'SQL' and 'Server'.
WinAudit.exe /r=g /o=ODBC /f=DRIVER=SQL Server;SERVER=PXSSQLSVR;UID=sa;DATABASE=winauditdb; /l=log.txt

Send a system overview to a MySQL database named winauditdb on the local computer using a DSN-Less connection string. Connect as root with a password.
WinAudit.exe /r=g /o=ODBC /f=DRIVER=MySQL ODBC 3.51 Driver;SERVER=localhost;UID=root;PWD=123456;DATABASE=winauditdb;

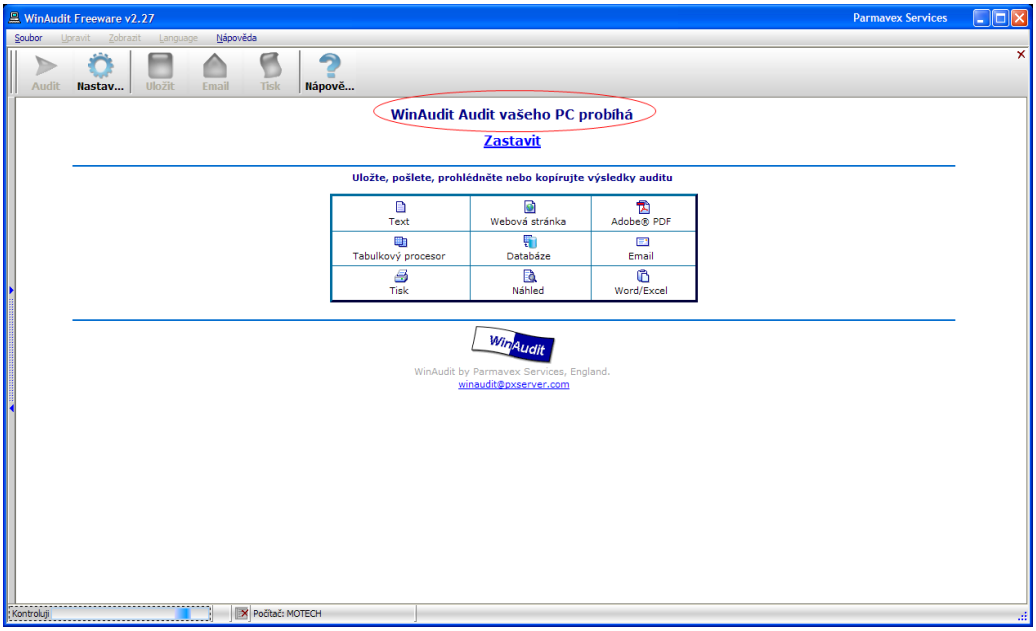
Uvítací okno aplikace:



Možnosti nastavení auditu programu WinAudit:



Zobrazené okno aplikace při průběhu kontroly počítače:



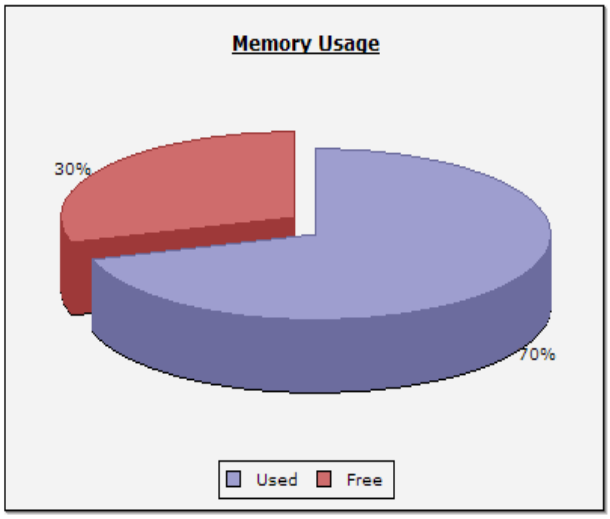
Výsledek auditu – informace o operačním systému testovaného počítače:

Operační systém

Name	Value
Name	XP
Edition	Professional
Install Date	18.12.2009
Registered Owner	Finanční úřad v Moravské Třebové
Registered Organization	Finanční ředitelství Hradec Králové
Product ID	[illegible]-23501
Major Version Number	5
Minor Version Number	1
Build Number	2600
Service Pack	Service Pack 3
Service Pack Version	3.0
Plus! Version Number	
DirectX Version	9.0c
Windows Directory	C:\WINDOWS\
System Directory	C:\WINDOWS\system32\
Temporary Directory	C:\DOCUME~1\[illegible]\LOCALS~1\Temp\

Informace o využití operační paměti testovaného počítače:

Paměť



Item	Value
Total Memory	1024MB (megabajtů)
Free Memory	315MB (megabajtů)
Maximum Swap File	2461MB (megabajtů)
Free Swap File	1918MB (megabajtů)

Obecné statistiky auditovaného počítače :

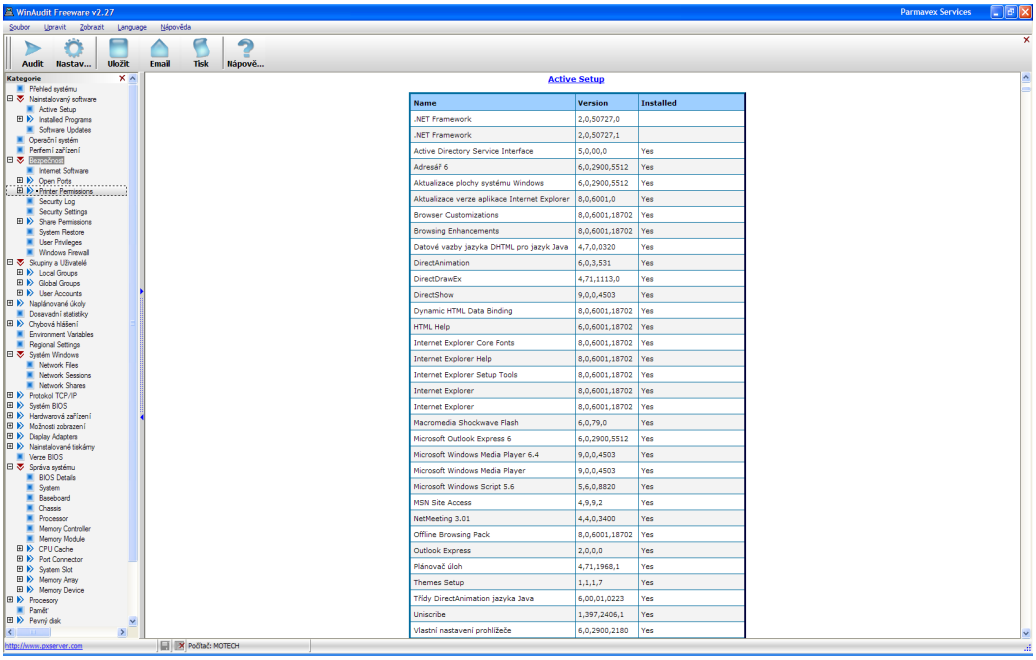
Naplánované úkoly

No Scheduled Tasks Found.

Dosavadní statistiky

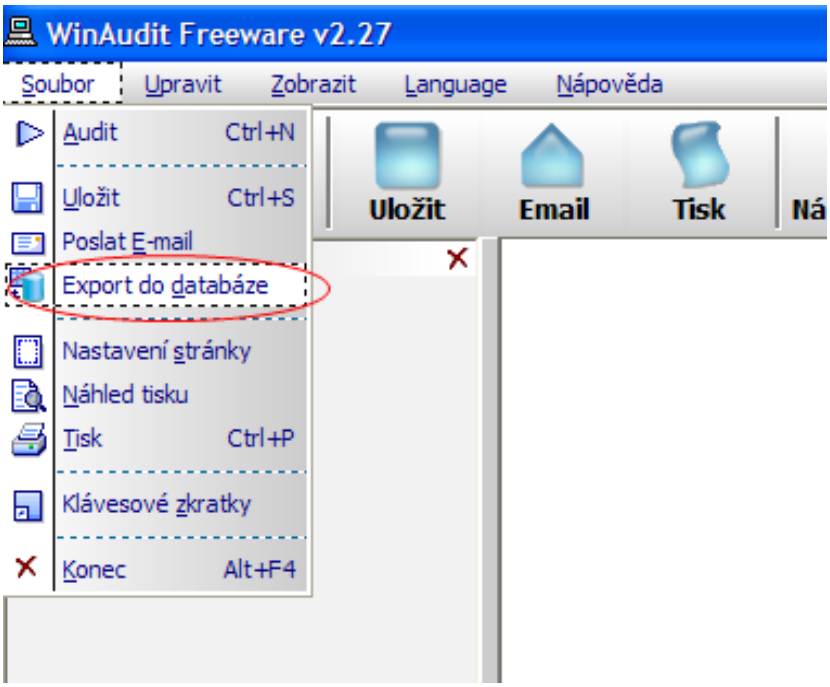
Name	Value
Data Start	27.1.2010 14:15:56
System Uptime	0 dní, 0 hodin, 11 minut
System Availability	7.640%
Total Uptime	4 dní, 19 hodin, 17 minut
Total Downtime	58 dní, 1 hodin, 44 minut
Times Booted	84
Clean Shutdowns	83
Unexpected Shutdowns	0

Kategorie auditu – záložky pro snadnější hledání požadovaných informací:

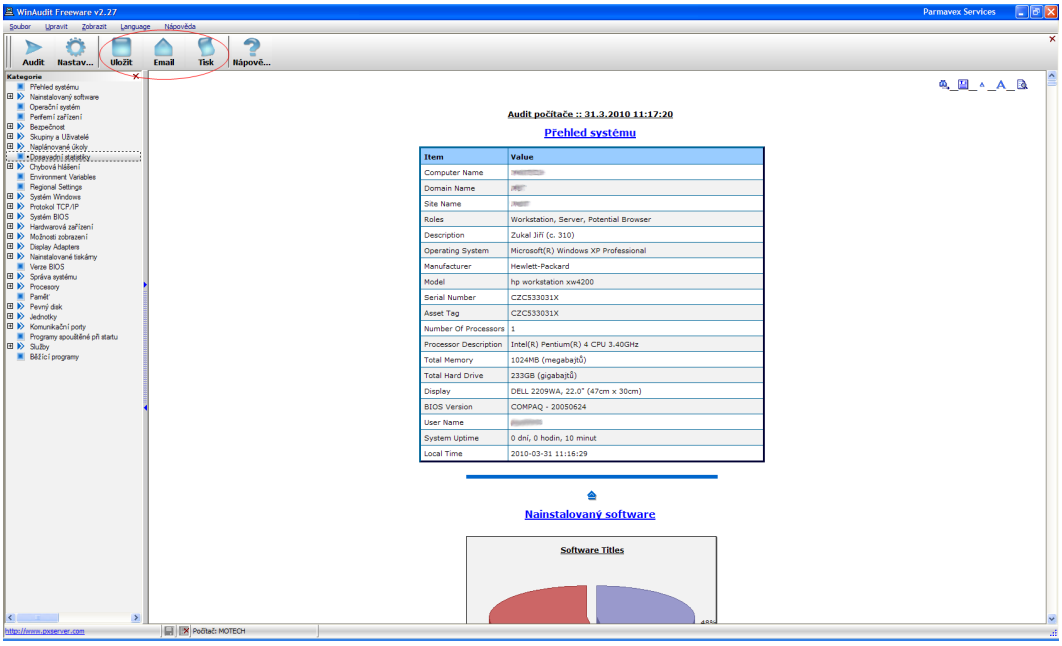


Name	Version	Installed
.NET Framework	2,0,50727,0	
.NET Framework	2,0,50727,1	
Active Directory Service Interface	5,0,00,0	Yes
Adresář 6	6,0,2900,5512	Yes
Aktualizace plochy systému Windows	6,0,2900,5512	Yes
Aktualizace verze aplikace Internet Explorer	8,0,6001,0	Yes
Browser Customizations	8,0,6001,18702	Yes
Browsing Enhancements	8,0,6001,18702	Yes
Datové vazby jazyka DHTML pro jazyk Java	4,7,0,0320	Yes
DirectAnimation	6,0,3,531	Yes
DirectDrawEx	4,71,1113,0	Yes
DirectShow	9,0,0,4503	Yes
Dynamic HTML Data Binding	8,0,6001,18702	Yes
HTML Help	6,0,6001,18702	Yes
Internet Explorer Core Fonts	8,0,6001,18702	Yes
Internet Explorer Help	8,0,6001,18702	Yes
Internet Explorer Setup Tools	8,0,6001,18702	Yes
Internet Explorer	8,0,6001,18702	Yes
Internet Explorer	8,0,6001,18702	Yes
Macromedia Shockwave Flash	6,0,79,0	Yes
Microsoft Outlook Express 6	6,0,2900,5512	Yes
Microsoft Windows Media Player 6.4	9,0,0,4503	Yes
Microsoft Windows Media Player	9,0,0,4503	Yes
Microsoft Windows Script 5.6	5,6,0,8820	Yes
MSN Site Access	4,9,9,2	Yes
NetMeeting 3.01	4,4,0,3400	Yes
Offline Browsing Pack	8,0,6001,18702	Yes
Outlook Express	2,0,0,0	Yes
Plánovač úloh	4,71,1968,1	Yes
Themes Setup	1,1,1,7	Yes
Třídy DirectAnimation jazyka Java	6,00,01,0223	Yes
Uniscribe	1,397,2406,1	Yes
Vlastní nastavení prohlížeče	6,0,2900,2180	Yes

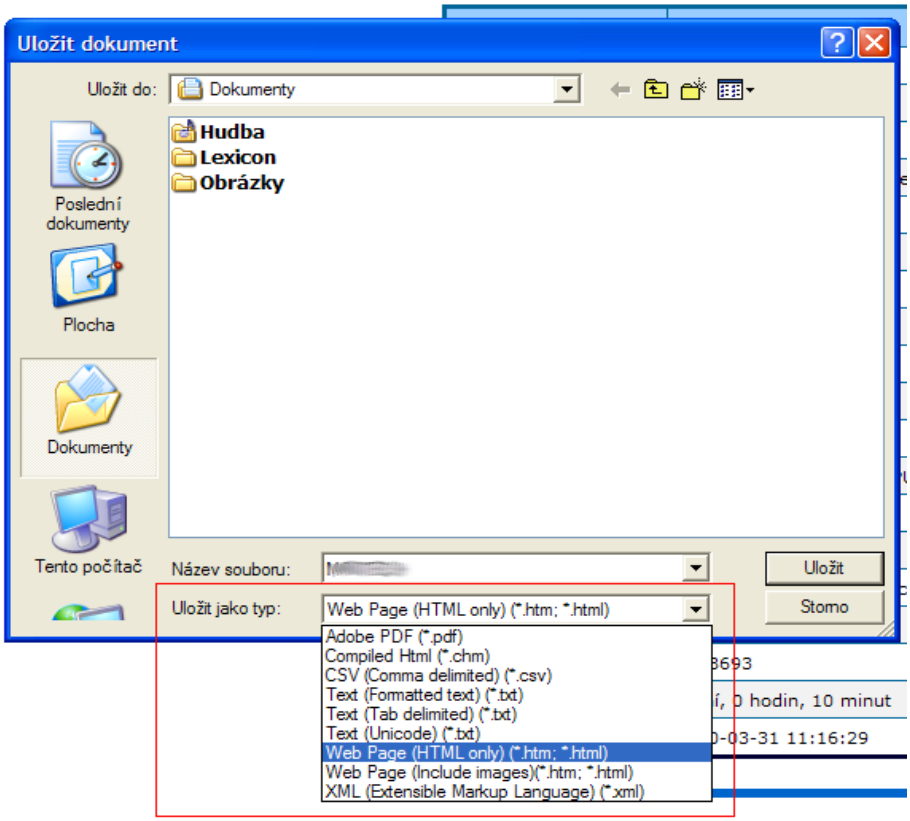
Volba exportu výsledků auditu do lokální databáze:



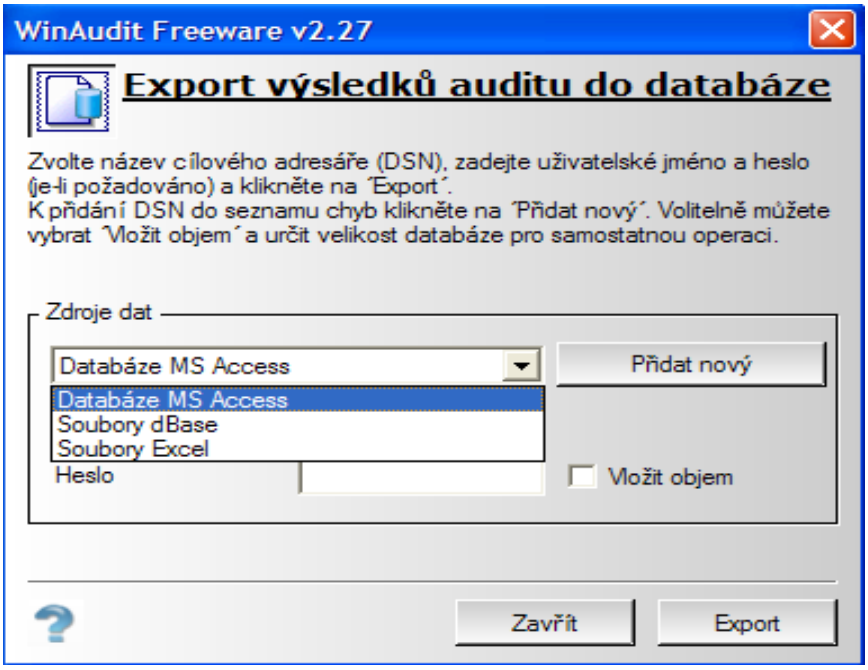
Obecný přehled o testovaném počítači:



Nabízené výstupní formáty souborů pro uložení výsledků auditu:



Možnosti exportu výsledků auditu do databáze:



Ukázka výsledku kontroly užití TCP/IP portů:

TCP 0.0.0.0:5900

Item	Value
Port Protocol	TCP
Local Address	0.0.0.0
Local Port	5900
Caption	TCP 0.0.0.0:5900
Service Name	
Remote Address	0.0.0.0
Remote Port	0
Connection State	Listening (LISTEN)
Process Name	C:\PCINFO\WinVNC.exe
Process ID	3892
Process Description	
Process Manufacturer	

Ukázka výsledku kontroly počítače – programy spouštěné po startu počítače:

Programy spouštěné při startu

Name	Settings Folder	Startup Command
ATIPTA	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\Program Files\ATI Technologies\ATI Control Panel\atiptaxx.exe"
FRYMXINS	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\Program Files\ATI Technologies\Fire GL 3D Studio Max\atiimxgl"
Smapp	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	C:\Program Files\Analog Devices\SoundMAX\SMTray.exe
ccApp	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
vptray	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	C:\PROGRA~1\SYMANT~1\VPTray.exe
Adobe Reader Speed Launcher	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
Adobe ARM	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
WinVNC	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\PCINFO\WinVNC.exe"
WinGrab	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\TESTY SW\WinGrab1.50\WinGrab.exe"
RegTool	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	C:\Program Files\Gemalto\Classic Client\BIN\RegTool.exe
Tweak UI	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RUNDLL32.EXE TWEAKUI.CPL,TweakMeUp
Cobian Backup 10 Interface	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"C:\Program Files\Cobian Backup 10\cbInterface.exe" -service
SmartDefrag	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	"I:\Install\AUTOINST\IDLE_DFRG\SmartDefrag\SD.exe" /StartUp
CTFMON.EXE	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	C:\WINDOWS\system32\ctfmon.exe
ManicTime	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	C:\TESTY SW\ManicTime\ManicTime.exe /minimized /name:
PTimer	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	"C:\TESTY SW\Sprinx Systems\Sprinx PTimer\PTimer.exe"
Hidden Administrator Server	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	C:\TESTY SW\Hidden Administrator\ha_server\ha_server.exe
ClocX	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	\\fumotnt3\abak\ClocX\ClocX.exe
desktop.ini	C:\Documents and Settings\All Users\Nabídka Start\Programy\Po spuštění\	
Microsoft Office.lnk	C:\Documents and Settings\All Users\Nabídka Start\Programy\Po spuštění\	
desktop.ini	C:\Documents and Settings\p608693\Nabídka Start\Programy\Po spuštění\	
Greenshot.lnk	C:\Documents and Settings\p608693\Nabídka Start\Programy\Po spuštění\	
OpenOffice.org 3.0.lnk	C:\Documents and Settings\p608693\Nabídka Start\Programy\Po spuštění\	

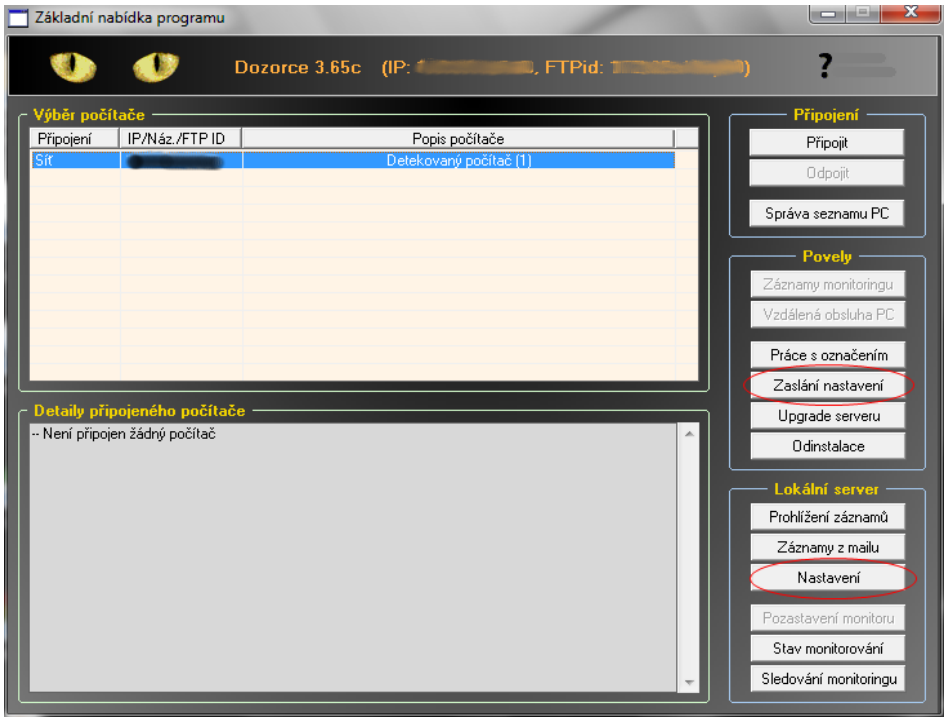
Obecné informace o verzi BIOS základní desky:

Verze BIOS

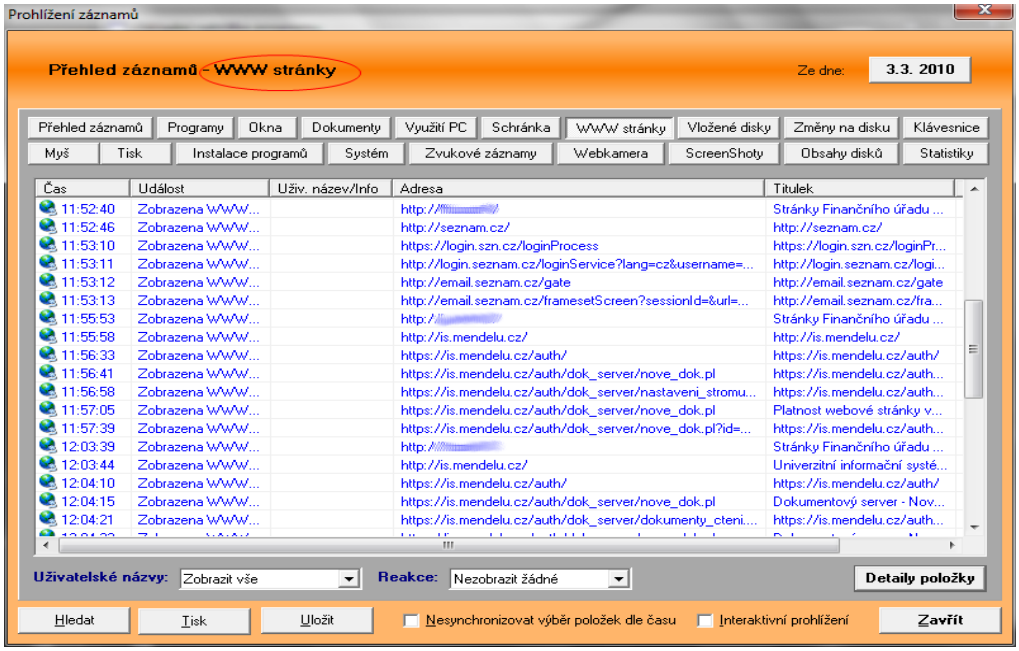
Name	Value
BIOS Version	COMPAQ - 20050624
Release Date	06/24/05
Video BIOS Version	
Video BIOS Date	04/12/02

PŘÍLOHA IV. : Monitorovací systém Dozorce

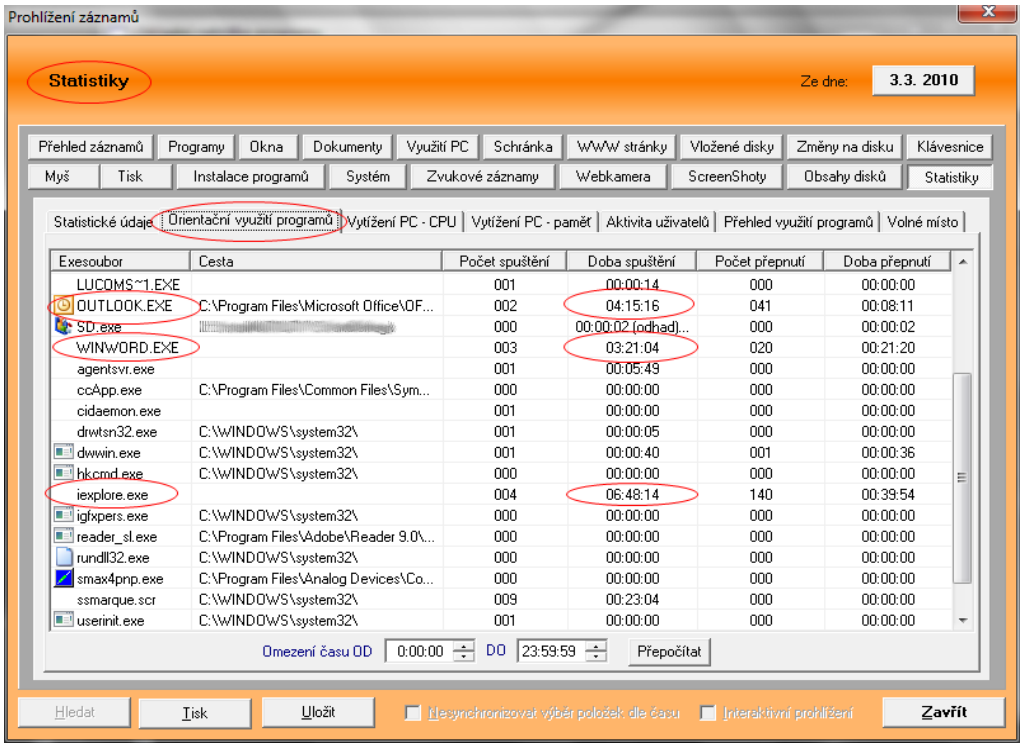
Okno aplikace – vzhled uživatelského rozhraní:



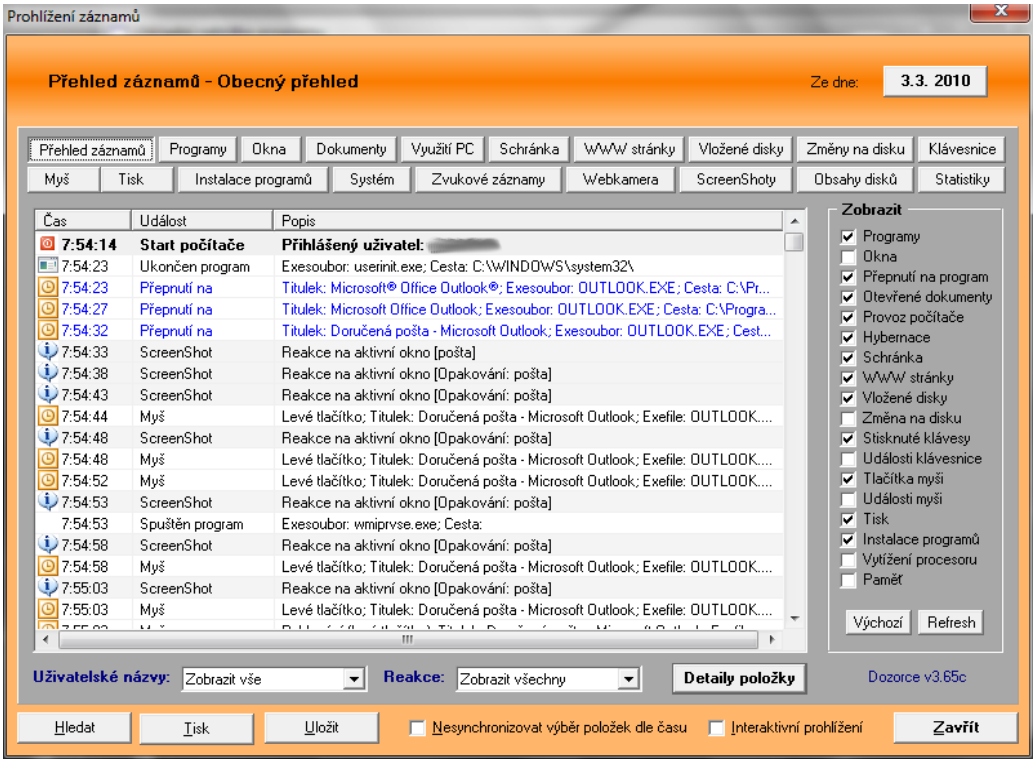
Seznam navštívených WWW stránek:



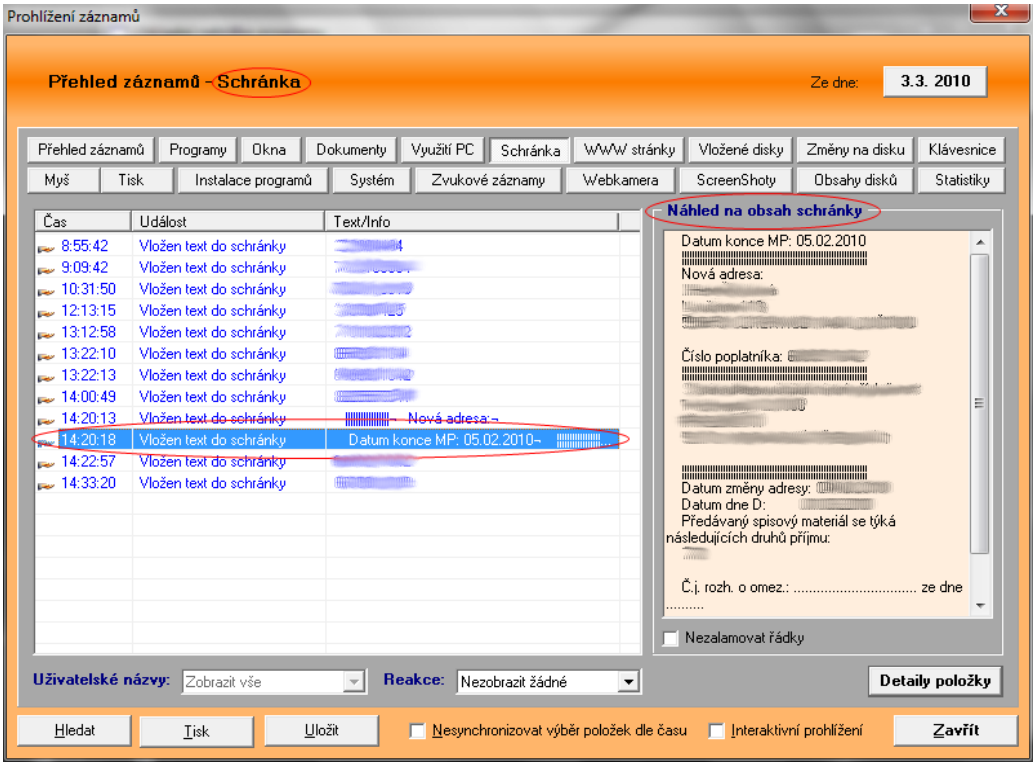
Okno pro prohlížení výsledků sledování – využití programů:



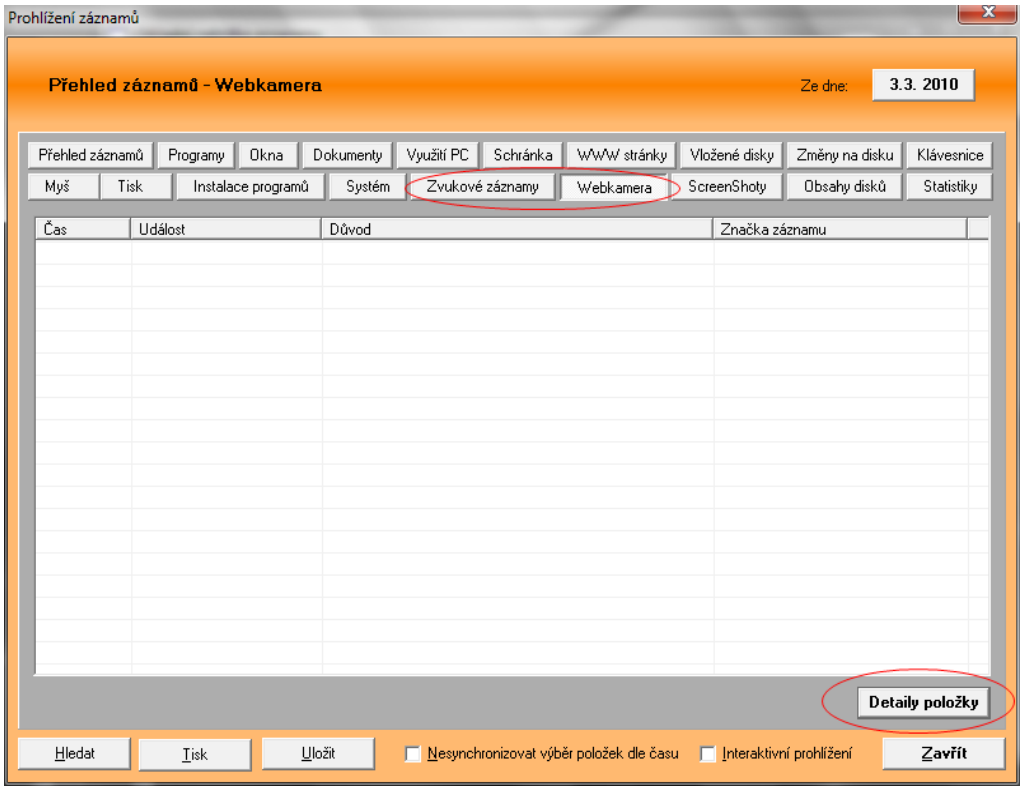
Přehled záznamů sledovaných událostí programu Dozorce:



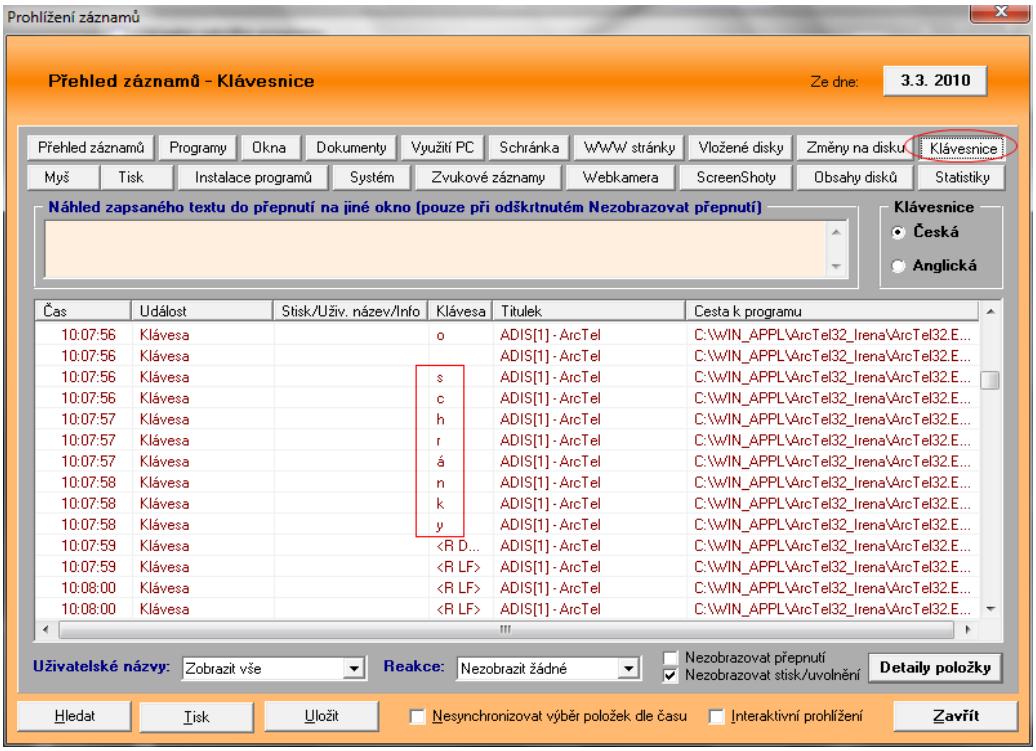
Záznamy o užívání schránky a její obsah:



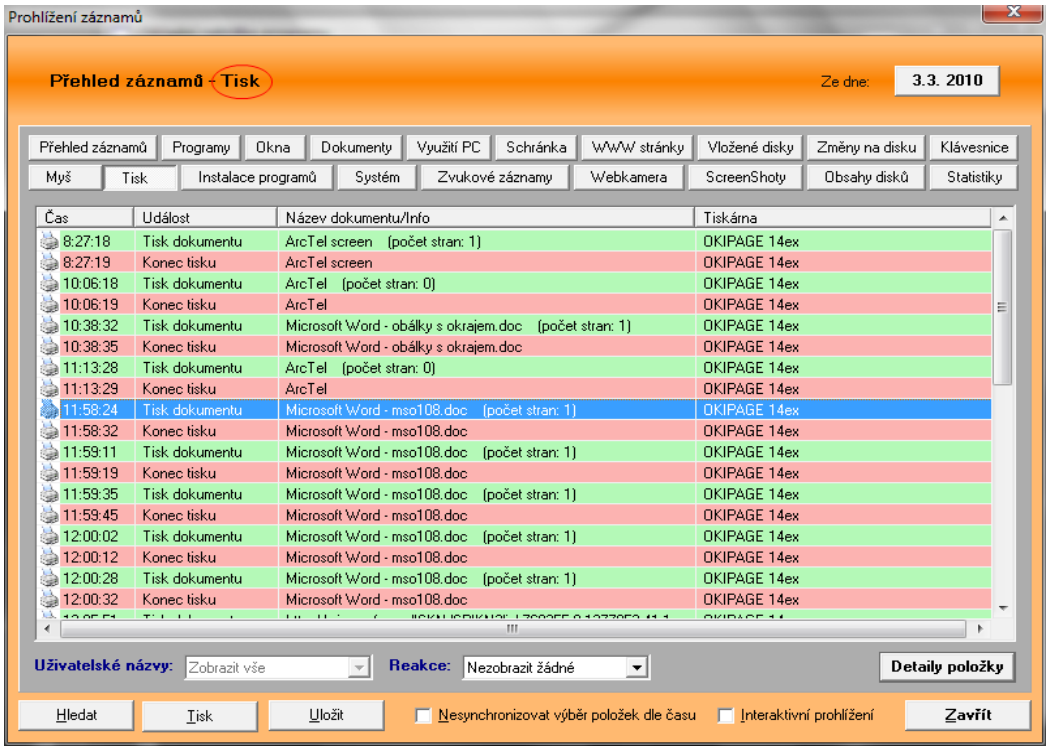
Možnost zachytávání zvukových streamů a záznamu z webkamery:



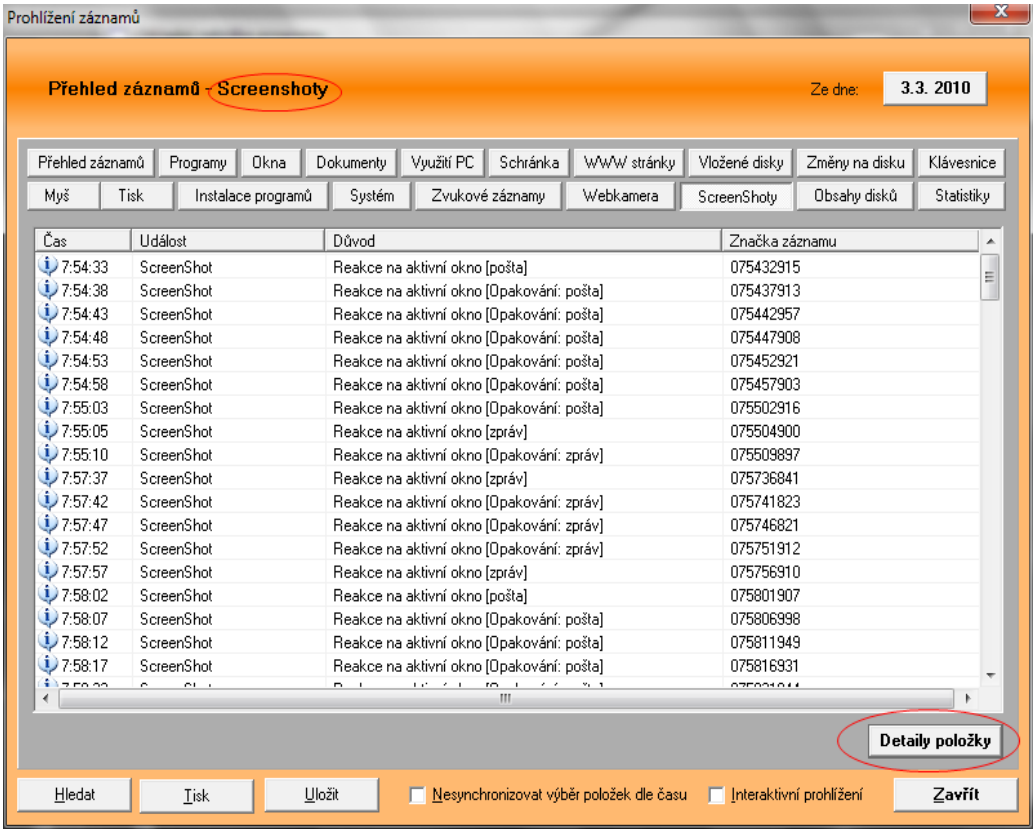
Ukázka záznamu zachytávání stisknutých kláves při psaní textu:



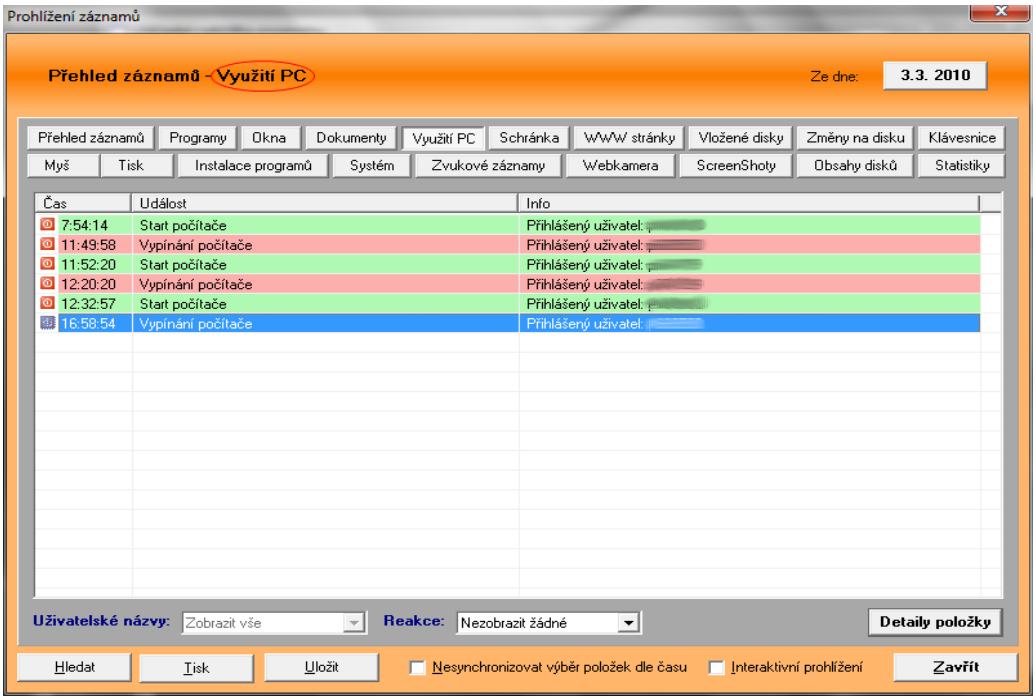
Záznam uskutečněných tiskových úloh:



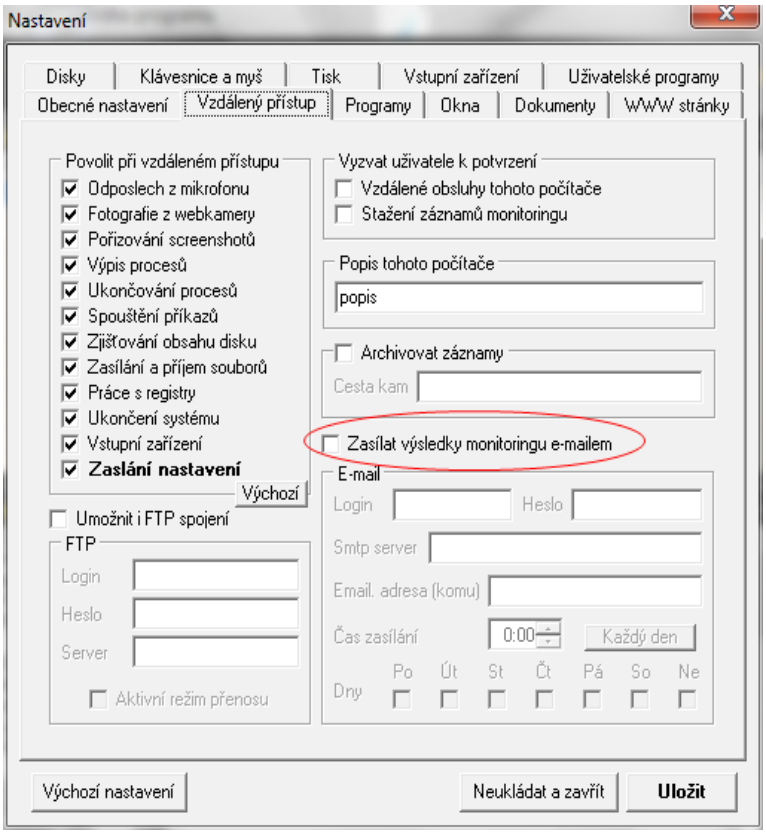
Seznam záznamů provedených otisků obrazovky:



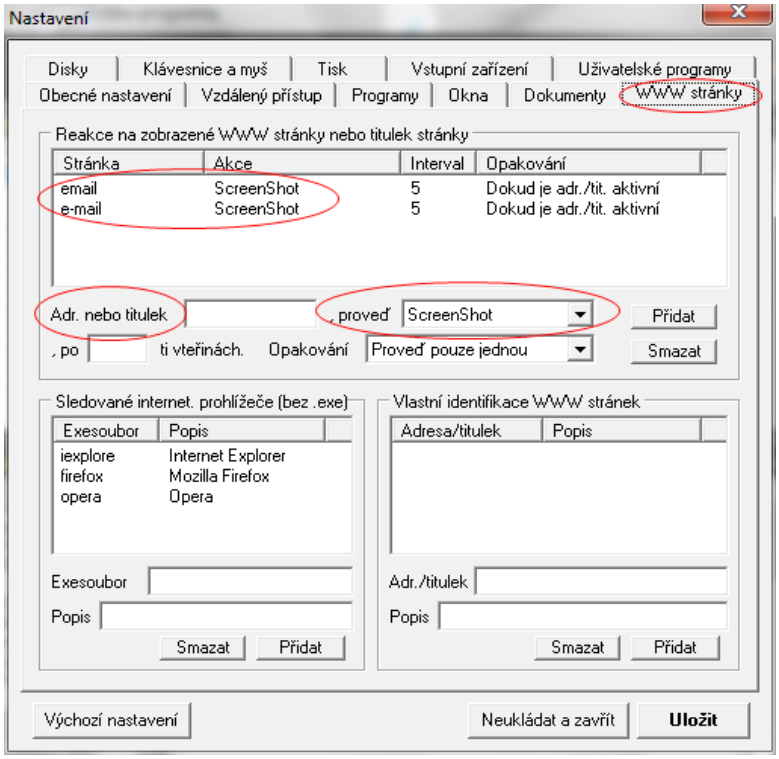
Využití počítače během pracovní směny – včetně restartů operačního systému:



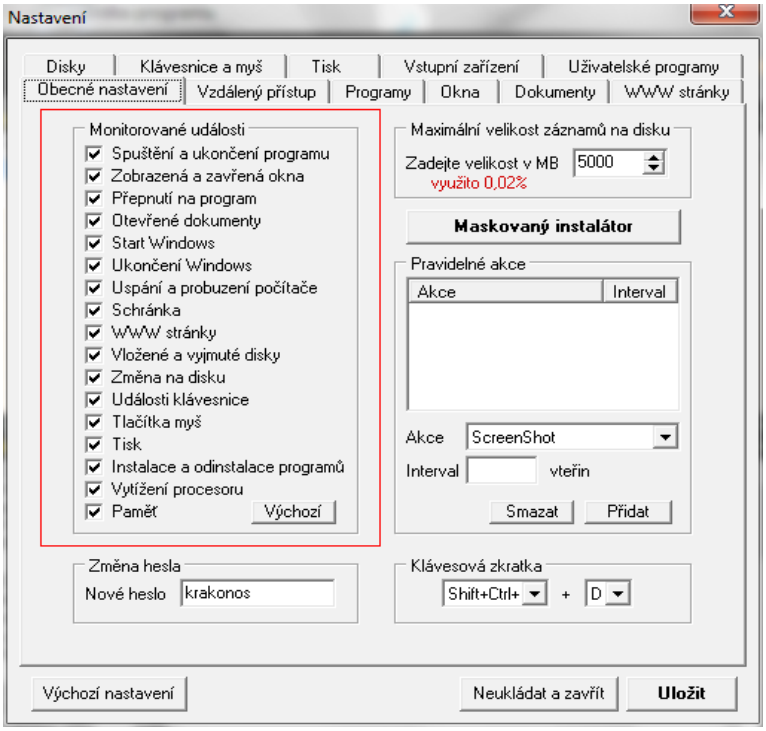
Nastavení vzdálené správy aplikace:



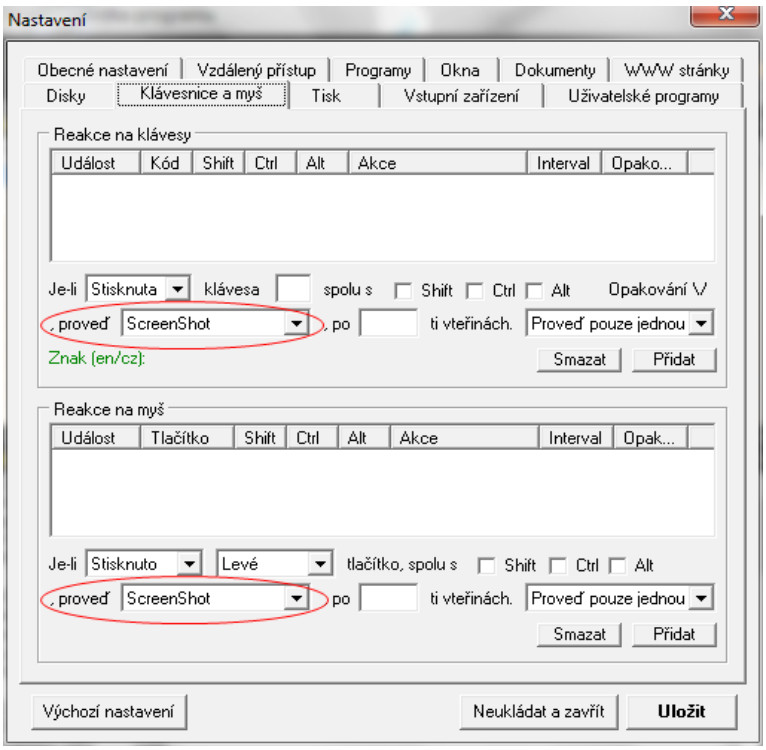
Možnosti nastavení parametrů sledování – prohlížení webu:



Nastavení hloubky sledovaní a jednotlivých činností:



Asociace akcí uživatele s procesem sledování jeho činností:



PŘÍLOHA V. : Kód pro odinstalaci klienta PCInfo MagicEYE

Obsah souboru *PCI_remove.bat* :

```
@echo off
rem    Davkovy soubor pro kompletni odinstalovani PCInfo klienta z pocitace
rem    urceny pro aplikaci v pripade, ze nejde spoustet audit na stanici s PCInfo klientem.

if not "%SystemDrive%"=="" goto WinNT
set SystemDrive=C:
if "%SystemDrive%"=="C:" goto WinNT

echo Davka NEMUZE POKRACOVAT!
echo Na Vasem pocitaci neni dostatek volneho mista v tabulce systemovych promennych.
echo Uvolnete prosim misto zrusenim nejake nepotrebne promenne, zvetsete prostor
echo pro tabulku systemovych promennych nebo upravte davku tak, aby pouzivala pevne
echo pismeno disku.
echo.
goto End

:WinNT
%SystemDrive%
cd\
attrib -r pcinfo.*
del pcinfo.*
rem del Pdoxusrs.net
if not exist PCINFO\nul goto Absent
cd PCINFO
if not exist winvnc.exe goto Next

start/wait winvnc -kill
start/wait winvnc -remove
del omnith~1.dll
del rda*.ver
del vnc.reg
del vnchooks.dll
del winvnc.exe
del zlib.dll

:Next
echo REGEDIT4 > $DelRC$.reg
echo [-HKEY_CURRENT_USER\AppEvents\EventLabels\VNCviewerBell] >> $DelRC$.reg
echo [-HKEY_CURRENT_USER\AppEvents\Schemes\Apps\VNCviewer] >> $DelRC$.reg
echo [-HKEY_CURRENT_USER\Software\ORL] >> $DelRC$.reg
echo [-HKEY_LOCAL_MACHINE\Software\ORL] >> $DelRC$.reg
echo [-HKEY_USERS\.DEFAULT\AppEvents\EventLabels\VNCviewerBell] >> $DelRC$.reg
echo [-HKEY_USERS\.DEFAULT\AppEvents\Schemes\Apps\VNCviewer] >> $DelRC$.reg
echo [-HKEY_USERS\.DEFAULT\Software\ORL] >> $DelRC$.reg
```

```
echo [-HKEY_LOCAL_MACHINE\Software\PCInfo] >> $DelRC$.reg
echo [-HKEY_CURRENT_USER\Software\PCInfo] >> $DelRC$.reg

start/wait regedit -s $DelRC$.reg
del $DelRC$.reg

if not exist hwinfo32.sys goto Next2
start/wait swinfo32 /UNINSTALL

:Next2
attrib -r -h pcinfo.dat
del pcinfo.dat
del *.exe
del *.ver
del *.aud
del *.pc?
del *.flg
del *.tmp
del *.$$$
del *.dll
del *.sys
del *.dat
del *.lng
del *.ini
del *.key
del *.reg
del *.pif
cd..
rd PCINFO
echo.

echo Soubory PCinfo klienta byly uspesne odstraneny.
echo.
goto End

:Absent
echo.
echo Na tomto pocitaci neni nainstalovan PCinfo klient.
echo.

:End
cd\
pause
```