POZOR! Co všechno o vás ví šéf!

David Čepička, Arne Arnold

Zabraňte nadřízeným sledovat, co děláte na svém počítači!

Váš šéf o vás ví takřka všechno! Není problém zjistit, na jakých stránkách se během pracovní doby pohybujete, s kým si dopisujete a jak moc na svém počítači skutečně pracujete. V našem článku vám prozradíme, jak se chránit před bedlivým okem zaměstnavatele.

Pokud si během pracovní doby vyřizujete na počítači své soukromé záležitosti, je jasné, že se to zaměstnavatelům moc líbit nebude. Takové jednání by vás také mohlo stát místo. Bylo zaznamenáno už několik případů, kdy se tak skutečně stalo, a výpověď byla posouzena jako oprávněná. V tomto článku vám ukážeme, jaké různé programy, tipy a triky může zaměstnavatel použít pro sledování počítače svých zaměstnanců a co všechno se může dozvědět.

Obecně totiž platí, že na používání počítače v zaměstnání k soukromým účelům právo nemáte. To samé platí i o využívání internetového připojení zaměstnavatele.

Nicméně vám v tomto článku poradíme, jak se proti podobnému sledování vašeho počítače chránit. Abyste však mohli naše tipy použít, musíte mít na vašem počítači v zaměstnání práva pro instalaci aplikací, což jinými slovy znamená, že u systémů Windows 2000 a XP musíte mít práva administrátora. To většinou nebývá pravidlem, a proto tam, kde to bude možné, vám prozradíme alternativní postupy pro uživatele bez administrátorských práv.

Nezapomeňte se vždy ujistit, že instalace softwaru není prohřeškem proti firemním pravidlům používání počítačů nebo proti některému ujednání ve vaší pracovní smlouvě. To samé platí i pro tipy, u nichž se sice žádný software neinstaluje, ale kdy by váš zaměstnavatel přesto mohl vaše počínání vyhodnotit jako prohřešek vůči smluveným pravidlům.

Server zaměstnavatele

Zkoušíte internetové aukce a máte políčeno na krásný fotoaparát s ještě zajímavější cenou. Jenomže dražba končí v 10 hodin. Nedá se nic dělat, musíte práci na několik minut přerušit a navýšit částku tak, abyste přístroj získali. Další příklad: chcete svému známému objednat v internetovém obchodě dárek, aby mu přišel přesně v den, kdy bude mít narozeniny. Takové aktivity bývají řadou zaměstnavatelů trpěny a řada zaměstnanců je zase bere jako samozřejmost. Přesto by všichni zaměstnanci měli mít na paměti, že z technického hlediska není sledování podobných aktivit pro zaměstnavatele žádný problém.

Surfování po internetu: jak lze sledovat zaměstnance

Prakticky v každé větší firmě je připojení k internetu řešeno tak, že se všichni zaměstnanci připojují prostřednictvím serveru, který slouží jako internetová brána. Tento server zpravidla ve standardním nastavení zaznamenává, kdy se který počítač připojil k internetu. Úroveň, v jaké mají být takové protokoly vedeny, se dá snadno nastavit. Pokud váš nadřízený bude chtít přesně vědět, co jeho zaměstnanci na internetu hledají, není pro něj problém použít nástroje, které mu to umožní zjistit. Řada takových utilit je dokonce dostupná zdarma. Příkladem může být třeba freewarový program **GFI Web Monitor** pro ISA Server od Microsoftu, který velmi přehledně vypíše informace o tom, který uživatel navštívil kterou stránku a jak často. Z komerčních produktů, které jsou zaměřeny na tuto oblast, můžeme zmínit kupříkladu **Surfcontrol Webfilter** nebo **Websense Enterprise**.

Ochrana tunelováním: nikým nerušené surfování

Protokolování všech vašich aktivit vedené na serveru zaměstnavatele ovlivnit sice nemůžete, nicméně můžete alespoň zabránit tomu, aby se server dozvěděl, které stránky navštěvujete. To zařídíte tak, že nebudete stránky vyvolávat přímo z vašeho počítače v práci, ale že si vybudujete tzv. tunel vedoucí z vašeho počítače přes firemní server k internetovým serverům. V tomto případě pak server vašeho zaměstnavatele zaregistruje pouze délku trvání tohoto připojení a množství přenesených dat. Vybudování tunelu bezpodmínečně vyžaduje na internetu nějaký koncový bod, který bude představovat konec tunelu. K dispozici máte dvě možnosti:

Vybudování tunelu zdarma: Pohodlným řešením, navíc ještě zdarma, je použití internetového anonymizéru. Doporučujeme vám kupříkladu použít utilitu **JAP**. Po instalaci utilita automaticky nakonfiguruje Internet Explorer tak, že budete moci automaticky surfovat anonymně. Jiné prohlížeče musíte bohužel konfigurovat sami. Pak budete surfovat prostřednictvím šifrovaného připojení, které správce firemního serveru nebude moci prohlížet.

Placený tunel: Program **HTTP Tunnel NG Client** připojíte po instalaci k serveru výrobce tohoto softwaru. Výhodou této utility je skutečnost, že nejen utajíte navštívené internetové stránky, nýbrž budete moci takové připojení používat i pro jiné aplikace. Vybudovaný tunel posílá data pouze přes port *80*. Z toho vyplývá, že můžete použít i takový software, který komunikuje na jiném portu, na němž by jinak firemní firewall komunikaci s největší pravděpodobností zablokoval. Pod tlačítkem *Configure Software* pak můžete zadat aplikace, pomocí nichž se budete připojovat k internetu - například **Internet Explorer** nebo třeba peer-to-peer klient **eMule**. Oblíbený Firefox bohužel podporován není.

A jak je to s cenou? Za komunikaci přenosovou rychlostí 15 KB za sekundu zaplatíte 1,49 USD měsíčně. Surfování touto rychlostí vám však mnoho radosti nepřinese. Rychlejší variantu připojení si můžete pořídit již za 4,99 USD měsíčně.

Při našem testování jsme mohli tuto službu používat několik dní zcela zdarma a bez přihlašování, ovšem při velmi malé šířce pásma.

Upozornění: Pokud si správce firemní sítě vybudovaného tunelu všimne, může zablokovat IP adresu serveru poskytujícího tunel, čímž vám spojení s tímto serverem znemožní.

Pro uživatele, kteří na svém počítači nedisponují právy administrátora a tudíž nemohou žádný software instalovat, se na internetové adrese *www.findnot.com* nabízí stejnojmenná internetová služba. V tomto případě se vytvoří tunel se zabezpečeným připojením prostřednictvím vašeho internetového prohlížeče. Velkou nevýhodou je cena; v současnosti musíte zaplatit za měsíc využívání služby 9,99 USD.

Připojení pomocí domácího počítače: Uživatelé, jejichž počítač je doma připojen k internetu pomocí trvalého připojení, mají ještě další možnost, jak si dosyta užít nerušeného surfování po internetu. Pomocí utility pro připojení vzdálené plochy navážete šifrované připojení mezi počítačem v zaměstnání a vaším počítačem doma. Pak uvidíte svůj domácí počítač na počítači zaměstnavatele přesně tak, jako kdybyste seděli před ním doma. Můžete používat prohlížeč a jiné utility vyžadující internetové připojení, aniž by firemní server dokázal toto připojení nějakým způsobem protokolovat. Jednou z aplikací, kterou vám pro tento účel rozhodně doporučujeme, je zdarma dostupný **Tight VNC**. Tuto utilitu nainstalujte na svůj počítač doma. Dříve než odejdete z domova do práce, připojte se k internetu a spusťte serverový modul Tight VNC z nabídky *Start/Programy/Tight VNC/TightVNC Server*. Při prvním spuštění programu změňte přístupové heslo a poté stiskněte tlačítko *Apply*. Toto heslo

budete potřebovat, až se budete v práci ke svému počítači připojovat. Budete také potřebovat IP adresu svého počítače.

Tu zjistíte, když klepnete myší na ikonku programu Tight VNC v pravé části hlavního panelu. Stejný software nainstalujte i na počítač v zaměstnání. Potom se připojte ke svému domácímu počítači klepnutím do nabídky *Start* na položku *Programy/TightVNC/TightVNC Viewer (Best Compression)*. Do políčka pro přihlášení zadejte poznamenanou IP adresu počítače a následně heslo. Poté uvidíte obrazovku svého domácího počítače a můžete jej ovládat, jak jste zvyklí.

Firemní server nyní bude zaznamenávat do svého protokolu data odpovídající připojení k vaší soukromé IP adrese. Tight VNC tato data přenáší nezašifrovaná. Správce firemního serveru může tato data zachytit a přečíst, i když je to poměrně náročná činnost. Pokud chcete přenášená data šifrovat, pak si přečtěte návod na internetových stránkách *www.tightvnc.com/faq.html*.

E-maily: Co všechno může administrátor přečíst

Ve většině firem je elektronická pošta vedena přes centrální poštovní server. Z tohoto důvodu není problém zaznamenat informace o odesílatelích, příjemcích a o předmětech zpracovaných e-mailů. I archivování všech e-mailů na serveru a náhled do jejich textů je velmi jednoduchý. Vaše e-maily tedy nejsou z technického hlediska pro vašeho zaměstnavatele ničím tajemným.

Ochraňte svoje e-maily před zvědavci

Nejlepší ochranou před zvědavci je šifrování e-mailů. K tomu účelu vám doporučujeme dva zdarma dostupné programy - **Gnu PP** a jednoduše ovladatelný **Ciphire**. V případě programu **Gnu PP** jsou však i přes šifrování údaje o odesílateli a příjemci stále čitelné.

Alternativou k šifrování je posílání soukromých e-mailů z nějaké jiné poštovní schránky, zřízené nejlépe na nějakém freemailovém serveru. Přitom však nesmí být taková poštovní schránka svázána s žádným z programů pro práci s elektronickou poštou (jako je například Outlook), protože komunikace přes protokoly POP3 nebo SMTP se dá velmi snadno vystopovat. Místo toho používejte webové rozhraní poskytovatele e-mailové schránky. Toto spojení je šifrované, takže je správce firemní sítě nebude moci číst a pozná pouze, že jste navštívili danou internetovou stránku.

Počítač na vašem pracovišti

Pokud chce šéf nasadit do kontroly vaší práce skutečně těžký kalibr, dozajista nalezne na internetu řadu skutečně vhodných kandidátů, pomocí nichž dokáže kompletně sledovat každý počítač. Špionážní programy tohoto typu obsahují keylogger a pravidelně vytvářejí screenshot. Ukládají vše, co vložíte do schránky pomocí klávesové zkratky <Ctrl><C>, dále ukládají hesla, jež zadáváte, navštívené internetové schránky, odeslané e-maily, sledují jak dlouho na počítači pracujete a evidují mnoho dalších informací.

Špionážní software na vašem počítači

Už dlouho se na trhu vyskytuje špionážní utilita **Spector Pro**. Tento program ukládá prakticky všechno, co se vůbec dá na počítači dělat, a posílá to přes počítačovou síť nebo prostřednictvím serveru SMTP ve formě e-mailu vašemu zaměstnavateli. Dalším programem je **Wiretap Professional**, který je k dostání za 49,95 USD. Ten rovněž zvládá kompletní kontrolu počítače. Ve své sharewarové verzi ovšem nedokáže utilita ukládat a odesílat žádné záznamy, které vytváří.

Jaké jsou šance proti špionážním programům

Profesionální špionážní utility se na vašem počítači dají rozpoznat jen velmi obtížně. Nejsou vidět ani ve Správci úloh, šifrují svoje záznamy a dají se na monitoru zobrazit pouze tajnou kombinací kláves.

Ovšem například **Wiretap Professional** přesto může zkušenější uživatel na svém počítači odhalit. Pokud spustí některý ze správců úloh systému Windows, jakým je kupříkladu **Process Explorer**, objeví tam proces SCVHOST.EXE. To však je velmi podezřelé, neboť systémový proces Windows se nazývá SVCHOST.EXE. Podobný název tedy ukazuje na pokus o skrytí nějaké položky. Jiné špionážní programy se ale maskují ještě lépe. Možná je najdete, pokud vyzkoušíte některé z těchto kroků:

1. Zkontrolujte, které spouštěcí soubory se automaticky nahrávají při startu Windows. To učiníte ve Windows XP pomocí programu MSCONFIG.EXE (klepněte na nabídku *Start/Spustit* a do políčka *Otevřít* napište daný příkaz).

2. Kontrolujte množství volného místa na pevném disku. Utilita pro sledování vaší aktivity na počítači vytvoří za den až 20 MB dat. Stačí tedy zkontrolovat množství dat ráno a odpoledne. Nezapomeňte však vzít v úvahu všechny vámi vytvořené soubory, dočasné soubory (vzniklé například při surfování na internetu), nové e-maily, stažené aktualizace programů, například u antivirů, a velikost odkládacího souboru.

3. Pozorujte objem dat přenesených počítačovou sítí. Pomůže vám zdarma dostupná utilita **MZL&Novatech Traffic Statistic**. Ta zaznamenává veškerou aktivitu počítačové sítě a zobrazuje v pravé části hlavního panelu přenesené objemy dat.

Sledování vašeho počítače prostřednictvím utilit pro dálkovou správu

Pro správce sítě jsou utility pro dálkovou správu velmi praktickou záležitostí. Pokud má někdo z pracovníků nějaký problém s počítačem, pak se některý z techniků může k jeho počítači připojit a hned vidí jeho pracovní plochu na svém počítači. Může daný problém okamžitě analyzovat a vyřešit. Utility pro dálkovou správu se však dají rovněž snadno zneužít pro sledování vašich aktivit. Pokud tedy vaše firma některý z programů tohoto druhu používá, pak by určitě měla být stanovena jasná pravidla v tom, co správce sítě dělat smí a co ne.

Forenzní analýza počítače

Tímto slovním spojením se myslí zkoumání počítače kriminalistickými metodami, kdy je cílem objevit a rekonstruovat již smazaná data, často proto, aby mohla posloužit jako elektronický důkaz o spáchání či nespáchání trestného činu. Provedení takové analýzy počítače není nikterak lacinou záležitostí, samozřejmě pokud ji provádějí profesionálové. Váš zaměstnavatel však za služby tohoto druhu určitě rád zaplatí, pokud mu byla například ukradena z počítače databáze důležitých zákazníků.

Specialisté na hledání dat vypátrají skoro každý bit

Máte-li důvodné podezření na krádež nějakých cenných dat, pak se můžete obrátit na některou z firem, zabývajících se tzv. forenzní analýzou. V České republice tyto služby poskytuje firma **Risk Analysis Consultants** (*www.rac.cz*).

Forenzní analýza začíná již v okolí samotného počítače. Sledují se i takové maličkosti jako umístění myši, protože z jejího umístění se dá usuzovat třeba na to, zda byl poslední uživatel počítače levák nebo pravák.

V dalším kroku se pořizuje přesný obraz pevného disku daného počítače a důkladně se prozkoumává každý bit. Tím se provede analýza všech na počítači se vyskytujících dat. Prostřednictvím speciálních utilit se pak zkoumá i oblast, na níž data uložena nebyla. Ta odpovídá volnému místu na pevném disku a obsahuje již smazané soubory. Kromě toho se rovněž získávají informace z tzv. *Slack Space* (viz tipy na okraji stránky). Zde se dají najít smazané a znovu přepsané soubory. Všechny nalezené informace se indexují pomocí utilit typu **Encase**, **Forensic Toolkit**, **Paraben** a dalších. Nakonec se v takto získaném indexovém souboru vyhledávají různá klíčová slova, která umožní dostat se k souborům, jež mohou zloděje dat odhalit.

Ochrana proti špiónům ve vašem počítači

Před zvědavými zraky svého nadřízeného se můžete chránit různými prostředky. Něco jiného ale je, pokud se váš počítač dostane do rukou některého z pracovníků zabývajících se forenzní analýzou. Ti totiž dokáží zjistit stopy vašeho počínání i přes použití zmíněných prostředků. Pokud byste chtěli zajistit, aby ani forenzní analýza neprozradila nic o vašich aktivitách během pracovní doby, pak by vás to stálo značnou dávku úsilí a ztratili byste při práci na počítači pocit jistoty a pohodlí. Například funkce *Obnovení systému* implementovaná ve Windows ME a XP ukládá řadu stavů, v nichž se váš počítač v jistých dnech nacházel. Vzhledem k tomu, že by se díky této užitečné funkci dalo objevit spousta stop vašich aktivit, museli byste funkci vypnout a při nějakém problému se systémem byste zůstali bez pomoci. Nejen z tohoto důvodu vám představíme pouze běžné postupy namířené proti špionáži ve vašem počítači.

Bezpečné odstraňování souborů: Chcete-li odstranit nějaký soubor, potřebujete k tomuto účelu skutečně kvalitní utilitu. Ta nejprve změní jméno a velikost odstraňovaného souboru. To je důležitá věc, neboť i po běžném odstranění tyto informace zůstávají na pevném disku. Potom následuje odstranění souboru a přepsání odstraněného souboru určitým počtem náhodných dat. Jednou z utilit, kterou můžeme k tomuto účelu doporučit, je **File Folder Cleaner**. Program obsahuje i komponentu **HD&D Cleaner**, která přepíše všechno volné místo na pevném disku, čímž spolehlivě zničí stopy i po dříve smazaných souborech. Položky v alokační tabulce disku odkazující na staré položky však neodstraní.

Odstranění stop po surfování na internetu a odstranění dočasných souborů: Windows a Internet Explorer ukládají informace o každém vašem výletu na internet. Internet Explorer sice nabízí možnost odstranění takových informací, ovšem ani zdaleka nemaže všechna data, která se během surfování uložila. Pro odstranění stop po surfování a pro vlastní odstranění souborů doporučujeme sharewarový program **Abylon Shredder**. Tento nástroj spolehlivě odstraní všechna potřebná data a její ovládání je velmi jednoduché. Velkým kladem utility je odstraňování dat dokonce i ze *Slack Space*. V programu se tato oblast nazývá *Clustertips*.

Několik rychlých tipů pro ochranu počítače proti sledování

V následujících řádcích vám přinášíme několik rychlých tipů, jak udržet svůj počítač čistý a jak zabránit zjištění stop po vašich soukromých aktivitách například na počítači v zaměstnání.

1. Surfujte anonymně

Neposkytujte firemnímu počítači žádné informace, na jakých stránkách internetu surfujete. Uděláte to tak, že začnete používat některý z tzv. anonymizérů, například program **JAP**.

2. Nezanechávejte po sobě stopy

Zahlaďte po sobě stopy. Skutečně důkladně to provedete prostřednictvím utility, která nejen maže data, nýbrž místo, které obsazovaly, několikrát přepíše. Velmi vhodná je například sharewarová utilita **Abylon Shredder**.

Pro odstranění dalších stop, například seznamu naposledy otevřených dokumentů, se nabízí **Ccleaner**. Program sice při odstraňování uvolněné místo nepřepisuje, jedná se ale o freeware a výhodou je jeho snadné ovládání.

3. Šifrování

Ukládejte svoje data na virtuální a šifrované pevné disky. Ty vytvoříte pomocí programu **Archicrypt Live**. Demoverzi, kterou nabízíme na našem CD, můžete používat 10 dní. Nabídne vám virtuální pevný disk o kapacitě 20 MB.

4. Fair Play

Zachovávejte pravidla hry, která platí ve vaší firmě. Pak se vám nemůže nic zlého stát.

Hardwarový keylogger

Keyloggery nemusí být vždy jen softwarové. Utility pro sledování vašich aktivit na počítači existují i v podobě samostatného hardwarového zařízení. Jedná se o malé zařízení, které se připojí mezi počítač a klávesnici. Takové zařízení dokáže uložit až 128 000 stisků, jež se následně po zadání určitého kódu dají přečíst. Jeho cena se pohybuje okolo 99 USD. Další informace naleznete na internetové stránce *keystroke- loggers.staticusers.net/hardware.shtml*.

Slack Space I

I již přepsaná data dokáží profesionálové obnovit. Jednotlivé soubory se totiž vyskytují na pevném disku v tzv. clusterech, což jsou vlastně nejmenší adresovatelné paměťové buňky. Velikost clusteru závisí na typu formátování disku a pohybuje se řádově v KB. Pokud má nějaký soubor například velikost pouhé 4 KB, je uložen v jednom clusteru, který má větší kapacitu. Takové neobsazené místo v clusteru pak může obsahovat data, náležející dříve smazanému souboru. Toto místo se nazývá *Slack Space*.

Slack Space II

V prostoru *Slack Space* se samozřejmě neukrývá velké množství dat. Přesto se zde dá při troše štěstí a náhody najít právě ta rozhodující část odstraněného e-mailu, kterou při forenzní analýze hledáme.

Jednoduché utility pro mazání dat, které přepisují i volné místo na pevném disku, se o *Slack Space* vůbec nezajímají. Data v těchto prostorech tak zůstávají i po několikerém použití takových utilit nedotčená.

Uvolněné místo

I když vysypete Koš ve Windows, zůstávají soubory na svém původním místě na disku. Jediným rozdílem je to, že první písmeno jména se v alokační tabulce pevného disku nahradí otazníkem. Tím operační systém zaznamená, že místo, které takový soubor obsazuje, je možné přepsat novým souborem - jedná se tedy o uvolněný prostor na disku. Pokud operační systém na takové místo žádný soubor neuloží, je možné smazaný soubor znovu obnovit, například pomocí utilit z řady **Easy Recovery**.

Přehled utilit pro špionáž a na ochranu proti ní

Program<T>**Kategorie**<T>**Cena**<T>**Operační systém**<T>**Internetová stránka**<T>**Název a velikost souboru**

Abylon Shredder 5.5<T>Utilita pro odstraňování souborů a složek<T>15,95 euro<T>Windows 95/98/ME, NT4, 2000, XP<T> **www.abylonsoft.com** a **na našem CD**<T>APMPROD.EXE, 10,1 MB

Archicrypt Live 4.8.1<T>Šifrování pevného disku<T>35 euro<T>Windows 98/ME, 2000, XP<T>**www.archicrypt-shop.com** a **na našem CD**<T> SETUPLIVE.EXE, 4,11 MB

Ccleaner 1.24.180<T> Utilita pro odstraňování souborů a složek<T>zdarma<T>Windows 95/98/ME, NT4, 2000, XP<T> **www.filehippo.com/download_ccleaner.html** a **na našem CD**<T> CCSETUP124.EXE, 503 KB

Ciphire 1.1.015<T>Šifrování e-mailů<T>zdarma<T>Windows 2000/XP<T> **www.ciphirebeta.com** a **na našem CD**<T> CIPHIRE-MAIL-1.1.015.EXE, 8 MB

Easy Recovery 6.1<T>Záchrana dat<T>od 45,24 euro<T>Windows 95/98/ME, NT4, 2000, XP<T>**www.ontrack.com/freesoftware** a **na našem CD**<T> ERPROT_610.EXE, 39,4 MB

File Folder Cleaner 2.2<T> Utilita pro odstraňování souborů a složek<T>zdarma<T>Windows 98/ME, 2000, XP<T> **home.pages.at/dragonsoftplanet/downloads/bayro/FFCsetup.exe** a **na našem CD**<T> FFCSETUP.EXE, 1,21 MB

GFI Web Monitor 3.0<T>Sledování surfování na internetu<T>zdarma<T>Windows 2000, 2003 Server<T>**www.gfi.com**<T>---

Gnu PP 1.1<T>Šifrování e-mailů<T>zdarma<T>Windows 95/98/ME, NT4, 2000, XP<T>**www.gnupp.com** a **na našem CD**<T>GNUPP-1.1-EN- INSTALLER.EXE, 3,09 MB

HTTP Tunnel NG Client 3.2<T>Utilita pro surfování na internetu<T>od 1,49 euro měsíčně<T>Windows 98/ME, NT4, 2000, XP<T>**www.http-tunnel.com** a **na našem CD**<T> HTTPTUNNEL_SETUP.EXE, 161 KB

JAP 00.05.022<T>Internetový anonymizér<T>zdarma<T>Windows 95/98/ME, NT4, 2000, XP<T>**anon.inf.tu- dresden.de/win/download_en.html** a **na našem CD**<T> JAPSETUP.EXE, 12, 5 MB

MZL&Novatech Traffic Statistic 1.2.0.1<T>Sledování sítě<T>zdarma<T>Windows NT4, 2000, XP<T>**www.trafficstatistic.com** a **na našem CD**<T>TRAFFICSTATISTIC_WIN_1.2.0.1.SETUP.EXE, 4,45 MB

Process Explorer 9.25<T>Správce procesů běžících ve Windows<T>zdarma pro soukromé použití<T>Windows 95/98/ME, NT4, 2000, XP<T>**www.sysinternals.com/Utilities/ProcessExplorer.html** a **na našem CD**<T> PROCESSEXPLORERNT.ZIP, 558 KB

Tight VNC 1.2.9<T>Vzdálené připojení plochy<T>zdarma<T>Windows 95/98/ME, NT4, 2000, XP<T>**www.tightvnc.com** a **na našem CD** <T>TIGHTVNC-1.2.9-SETUP.EXE, 944 KB

Spector Pro 5.0<T>Sledování počítače<T>99 dolarů<T>Windows 98/ME, NT4, 2000, XP<T>**www.spectorsoft.com**<T>---

Surfcontrol Webfilter<T>Sledování surfování na internetu<T>na dotaz<T>Windows 2000, 2003 Server<T>**www.websense.com**<T>---

Websense Enterprise 5.5<T> Sledování surfování na internetu<T>na dotaz<T>Windows 2000, 2003 Server, Linux<T>**www.websense.com**<T>---

Wiretap Professional 4.0<T>Sledování počítače<T>shareware(49,95 dolarů plná verze)<T>Windows 98/ME, NT4, 2000, XP<T> **www.wiretappro.com** a **na našem CD**<T>WIRETAPPRO.EXE, 1,86 MB