Co všechno o vás ví váš šéf

Váš nadřízený se o vás pomocí **ŠPIONÁŽNÍCH NÁSTROJŮ** může dozvědět mnohé: jaké posíláte soukromé e-maily, které webové stránky navštěvujete, komu voláte. Chip vám prozradí, jak se takovému „dohledu“ bránit.

FABIAN VON KEUDELL

V celé řadě firem už tato činnost probíhá celé roky a s největší pravděpodobností se něco podobného děje i u vás. Když si vás šéf zavolá „na kobereček“, bývá už obvykle dobře připraven – ví, kdy začínáte pracovat, jak často píšete soukromé e-maily a kdy surfujete na internetu.

Špionážní nástroje dokáží o každém, kdo pracuje na počítači, zjistit téměř vše. Software také vypočítává „efektivní“ pracovní dobu. Tato technologie není nová: monitorující software byl vyvinut pro administrátory. Ti mají přístup k jakémukoliv počítači v síti i přes „vzdálenou plochu“. Mohou počítač nejen vzdáleně ovládat (což se např. využívá pro instalaci zabezpečovacích nástrojů či záplat), ale dokáží také monitorovat, co se na něm v každém okamžiku děje.

V současné době je monitoring o mnoho jednodušší, protože potřebné funkce jsou integrovány téměř ve všech moderních operačních systémech. Vzdálenou plochu najdete ve Windows XP, ve Vistě je špionáž usnadněna tzv. „rodičovskou kontrolou“ (funkce Parental Control, která ale může kontrolovat i dospělé – například zaměstnance).

Běžná praxe: Špionáž je jednoduchá

Pomocí několika příkladů vám ukážeme, jak jednoduché je monitorovat zaměstnance, aniž by měli sebemenší náznak podezření. Program Boss Everyware (**www.bosseveryware.com**) se neprozradí žádnou ikonou na ploše ani v „system tray“, a neprozradí se dokonce ani ve Windows Task Manageru. Čmuchala můžete odhalit pouze pomocí speciálních nástrojů, jako je Process Explorer. Obvykle se takhle dobře dokáží maskovat pouze viry a malware.

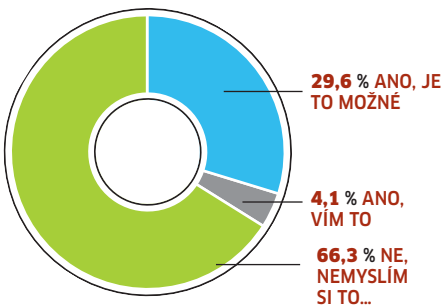
Program Boss Everyware není jediným zástupcem programů, jejichž jméno cosi napovídá o jejich účelu. Také další digitální špioni vám svým názvem naznačují, čím se v systému zabývají – viz například špionské nástroje Spector Pro, WinWhatWhere nebo Spy Agent.

Průměrná cena špionážního programu se pohybuje mezi 50 a 70 eury. Jednotlivé programy se od sebe moc neliší: obvykle dokáží zaznamenávat všechny stisky kláves, vytvářet v pravidelných intervalech snímky obrazovky a ukládat seznam používaných programů a navštívených webových stránek.

Jejich instalace je stejně jednoduchá jako monitoring. Pracovní špioni jsou buď zasláni přes e-mail (a využívají metody obvyklé pro viry), nebo vám systémový administrátor přímo z firemní sítě nainstaluje software na počítač. Programy si poté samy vytvoří položky zabezpečující automatický start při zapnutí počítače. Šéf si pak může zvolit monitoring podle své chuti a potřeb: jak často má nástroj ukládat snímky obrazovky, která klíčová slova má hlídat ve vybraných aplikacích (například v e-mailu nebo v instant

Špionážní průzkum

Chip se ptal zaměstnanců pracujících na PC: Myslíte si, že jste v práci tajně monitorováni? Třetina dotázaných odpověděla „Ano“...



ZDROJ: PRŮZKUM GFK (ZADÁNÍ CHIP)

NAJDETE NA DVD

Antišpionážní nástroje

AntiVir Personal Edition ► Bezplatný antivirový program

Firestorm ► Odstraňuje špionážní programy

JAP ► Nabízí anonymní surfování na internetu

LocateProtect ► Chrání před nežádoucí „mobilní detekcí"

SpyBot – Search&Destroy ► Nedá šanci většině spywaru

SpywareBlaster ► Hledá na vašem počítači „čmuchaly"

Spyware Terminator ► Hledá a odstraňuje nežádoucí software

X-Ways Trace ► Seznam stop po vašich toulkách internetem

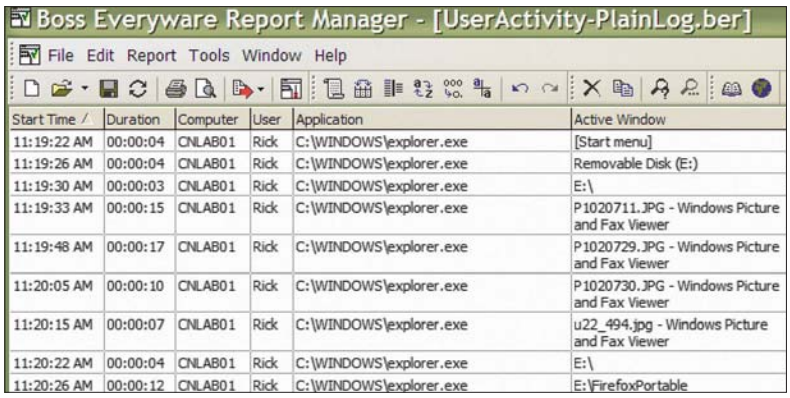
► **NA DVD:** Programy k článku najdete na DVD pod indexem **ŠPION V PRÁCI**

messengerech) – a to vše jen pomocí pár kliknutí v nastavení programu.

Výrobce programu Boss Everyware slibuje čmuchalským šéfům získání všech informací o zaměstnancích: jak dlouho a na jakých stránkách v pracovní době surfovali, kolik času strávili posíláním soukromých e-mailů, jak dlouho si povídali s kolegy přes ICQ...

Programátoři také používají speciální triky, aby monitorovací programy zůstaly před běžnými nástroji proti malwaru skryty. Stránky výrobců často obsahují instrukce pro nastavení nejznámějších antispywarových nástrojů – návod, jak a které funkce v bezpečnostních programech deaktivovat. Mnohdy je to poněkud absurdní taktika – ve jménu špionáže snižují zabezpečení počítače...

Tyto aktivity však mohou zajít i dál. Například na webové stránce produktu Spector Pro je ukázka, jak lze nástroj využít k „ochraně počestnosti domu". Muž předvádí, jak používá nástroj Spector k monitorování aktivit vlastní dcery – například čtení její konverzace na chatu. Další kupec se chlubí tím, že díky čmuchalskému programu může vyhodit deset procent zaměstnanců. Jedná se o výjimečné případy nedůvěřivých otců a šéfů? Bohužel ne. Studie auditorské firmy PricewaterhouseCoopers odhaluje, že 85 procent všech britských zaměstnavatelů monitoruje své zaměstnance. U nás je ale toto procento z celé řady důvodů o dost nižší...



Start Time	Duration	Computer	User	Application	Active Window
11:19:22 AM	00:00:04	CNLAB01	Rick	C:\WINDOWS\explorer.exe	[Start menu]
11:19:26 AM	00:00:04	CNLAB01	Rick	C:\WINDOWS\explorer.exe	Removable Disk (E:)
11:19:30 AM	00:00:03	CNLAB01	Rick	C:\WINDOWS\explorer.exe	E:\
11:19:33 AM	00:00:15	CNLAB01	Rick	C:\WINDOWS\explorer.exe	P1020711.JPG - Windows Picture and Fax Viewer
11:19:48 AM	00:00:17	CNLAB01	Rick	C:\WINDOWS\explorer.exe	P1020729.JPG - Windows Picture and Fax Viewer
11:20:05 AM	00:00:10	CNLAB01	Rick	C:\WINDOWS\explorer.exe	P1020730.JPG - Windows Picture and Fax Viewer
11:20:15 AM	00:00:07	CNLAB01	Rick	C:\WINDOWS\explorer.exe	u22_494.jpg - Windows Picture and Fax Viewer
11:20:22 AM	00:00:04	CNLAB01	Rick	C:\WINDOWS\explorer.exe	E:\
11:20:26 AM	00:00:12	CNLAB01	Rick	C:\WINDOWS\explorer.exe	E:\FirefoxPortable

Rozšířené informace: Špionážní nástroj Boss Everyware může pomoci vašemu šéfovi zjistit, které programy jste spouštěli, kdy a jak dlouho jste je používali...

Jednoduše: Ochrana pomocí standardních nástrojů

Máte pocit, že jste monitorováni, a zároveň vám není dovoleno nainstalovat si software, který by mohl demaskovat čmuchaly na vašem PC? Žádný problém! V mnoha případech dokáže špiony odhalit i „obyčejný" Windows Explorer. Pro obtížné případy budete ale potřebovat dodatečné nástroje. Malý zádrhel spočívá v tom, že ačkoliv jsou tyto nástroje k dispozici zdarma, pro jejich správnou funkci jsou nutná administrátorská práva. Při testování těchto nástrojů pak nezapomeňte, že monitorovací software za-

INTERVIEW

Monitorování zaměstnanců na pracovišti: Kde jsou jeho skutečné meze?

Práva zaměstnanců a zaměstnavatelů v oblasti užívání firemních počítačů jsou pro většinu z nás velkou neznámou – na čí straně je ve skutečnosti zákon? Zeptali jsme se na toto téma jedné z předních advokátních kanceláří v České republice, která se ve své praxi zaměřuje mimo jiné i na právo informačních technologií a otázky zaměstnanosti a pracovních vztahů.

Mgr. Marie Janšová, advokátní kancelář Glatzová & Co. (www.glatzova.com)

1) Může zaměstnavatel monitorovat činnost zaměstnance na počítači (například monitorováním stisku každého tlačítka)?
Problematika monitorování zaměstnanců na pracovišti je stále velmi diskutovaná. Její podstata tkví v co možná nejideálnějším vyvážení práva na soukromí zaměstnance a práva zaměstnavatele na to, aby zaměstnanec využíval pracovní dobu jen k práci a nezneužíval majetek firmy k soukromým účelům, či dokonce firmu přímo nepoškozoval. Právní předpisy jednoznačně stanoví, že zaměstnanec nesmí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní ani pracovní prostředky zaměstnavatele včetně výpočetní techniky či telekomunikačních zařízení. Dodržování tohoto zákazu je pak zaměstnavatel oprávněn kontrolovat. Firma může určit, jakým způsobem a v jakém rozsahu se budou využívat její pracovní prostředky, tak aby bylo dosahováno nejefektivnějšího výkonu práce. Kontrola však musí být přiměřená a odůvodněna závažným zájmem zaměstnavatele. Tím je např. zájem na ochraně know-how, databáze zákazníků, výrobních postupů aj. V oboru bankovnictví je závažným důvodem například přísná ochrana zájmů třetích osob. Zde by mohlo být ospravedlnitelné i použití „keylogeru" nebo monitorování obrazu. Obecně pak lze říci, že přiměřenou kontrolou je např. monitorování spuštěných aplikací na počítači, kontrola obsahu paměti, způsob užívání počítače, jinými slovy kolik času stráví zaměstnanec na internetu a na jakých webových stránkách se pohybuje.

2) Může zaměstnavatel blokovat konkrétní WWW stránky?
V zablokování konkrétních webových stránek nevidím žádný právní problém. Naopak toto je v souladu s oprávněním zaměstnavatele určit rozsah užívání pracovních prostředků.

3) Má zaměstnavatel povinnost informovat své zaměstnance o tom, že jsou při práci monitorováni?
Ano, zaměstnanci musí být o tom, že jsou takovýmto způsobem v práci kontrolováni, resp. o způsobu dohledu nad využíváním pracovních prostředků předem informováni. Monitorování, o kterém by zaměstnanec nevěděl, by bylo možné považovat za nepřiměřený zásah do jeho osobnostních práv.

4) Může šéf číst mé e-maily?
Tato otázka má dvě roviny – první je čtení korespondence z firemní e-mailové schránky a druhou pak čtení ze schránky soukromé, pouze otevřené na pracovním PC. Pokud jde o schránku firemní a ta je takto i jasně vymezená při jejím předání zaměstnanci, je tato schránka stále vlastnictvím zaměstnavatele, stejně jako pošta v této schránce. Zaměstnanec je pak jen jejím uživatelem a každý e-mail z ní odeslaný je zasílaný jménem zaměstnavatele a příchozí e-mail je určen opět společnosti (zaměstnavateli). Zaměstnanec jej pouze zpracovává. Do takovéto schránky pak má podle mého názoru zaměstnavatel přístup a může ji kontrolovat. Pokud by však v ní objevil zjevně osobní e-mail zaměstnance, měl by ji zavřít, nepokračovat ve zkoumání jejího obsahu a vyzvat zaměstnance, aby tento e-mail neprodleně odstranil. Případně by mohl řešit postih zaměstnance, že pracovní pomůcku neužívá v souladu s pracovními předpisy. Pokud se jedná o kontrolu osobní e-mailové schránky, kterou si zaměstnanec otevře na pracovním počítači, pak taková kontrola v žádném případě možná není. Pouze, stejně jako v předchozím případě, by zaměstnavatel mohl zaměstnance postihnout za to, že neužívá pracovní pomůcku v souladu s pracovními předpisy, příp. v pracovní době vyřizuje soukromé záležitosti. Konkrétní postup však bude záležet zejména na právních a etických pravidlech každé firmy. Lze doporučit jasné vymezení funkcí pracovní e-mailové schránky a vytvoření speciální schránky pro soukromou poštu či její zřízení jinde.

INFO

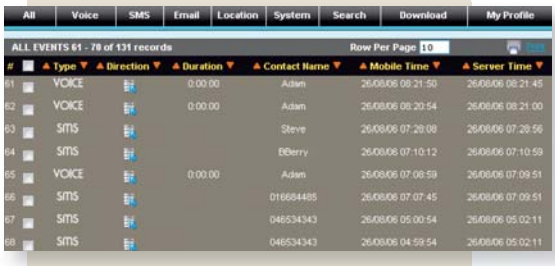
Mobilní telefon jako štěnice

Šéf může pomocí speciálního softwaru monitorovat i telefony zaměstnanců...

Špionáže se nezbavíte, ani pokud vám firma nabídne mobilní telefon: po nainstalování speciálního softwaru (např. FlexiSpy) se z něj totiž stane totální zrádce. Tento špionážní nástroj je obzvláště protivný: dokáže zaznamenat všechna data (obsah odeslaných SMS, čas a délku hovoru včetně jména volaného) a uložit je na webovou stránku. Na ní si může váš šéf přímo ze svého počítače prohlédnout vaše „telefonní aktivity". Navíc, pokud bude chtít, může poslouchat i libovolné hovory – aniž byste si čehokoliv všimli, špionážní program nepozorovaně vytvoří spojení.

Proti tomuto typu špionáže je jediná ochrana – použití mobilních virových skenerů (například Norton Smartphone Security nebo Kaspersky Mobile Security).

Jestliže si ale myslíte, že vám k anonymitě pomůže vlastní smazání „zrádných" stop (volaných čísel a odeslaných SMS), jste na velkém omylu. Jediné, co šéf potřebuje, je program Cell Phone Spy Data Extraktor od firmy BrickHouseSecurity (**www.brickhousesecurity.com, 95 eur**). Tento program dokáže zjistit i bezpečnostní PIN telefonu a v současné době proti němu neexistuje účinná obrana.



Špehování s FlexiSpy: Šéf může vidět všechna data na webové stránce.

znamenává každou činnost – i spuštění těchto nástrojů.

Řešení tohoto problému ale existuje. Většina špionážních programů nabízí přímý přístup ke konfiguraci pomocí klávesových zkratek, které administrátoři používají k nastavování „čmuchání". Pokud budete mít štěstí, budou tyto zkratky nezměněné. V každém případě ale můžete vyzkoušet kombinace, které jsou uvedeny v tabulce. Špionážní aplikace také můžete často poznat podle souborů nainstalovaných v systému.

Pro hledání souborů stačí použít klasické vyhledávání Windows – pouze se ujistěte, že máte aktivováno vyhledávání skrytých souborů. Soubory, které byste se měli pokusit najít, také najdete v již zmiňované tabulce. Pokud jste odhalili přítomnost špionážního programu, ve většině případů ho můžete odstranit pomocí antivirového programu. Nepodaří-li se to, musíte ho vymazat manuálně. Instrukce najdete na internetu – stačí jen vložit do Googlu název programu a slovo „remove".

Nejlepší nástroje: Sbohem, špionáži

Z hlediska obrany proti špionáži poslouží i jinak poněkud neschopný Windows Defender. Ačkoliv nedokáže udržet tempo s komerčními virovými skenery, nabízí užitečné nástroje, které pomáhají při vyhledávání špionážních programů. Stáhněte si ho z webu Microsoftu **www.microsoft.com/downloads**. Poté, co si tento nástroj nainstalujete, měl by vás upozornit na každé potenciální ohrožení ze strany spywaru. Jak jsme se ale přesvědčili v jednom z minulých Chipů, nikdo není dokonalý, a tak by bylo poněkud lehkomyslné spoléhat se pouze na něj. Windows Defender však přesto nabízí praktický a přitom méně známý nástroj, který vám pomůže nalézt spyware. Tento nástroj najdete ve v sekci »Tools | Software Explorer«. Klíčovým pomocníkem je zde sekce „Startup Programs", která odhalí všechny programy spouštějící se automaticky při bootování Windows. Klikněte na název programu a získáte detailní informace například o jeho umístění na disku nebo datum instalace. Najdete-li podezřelý soubor, bezbolestně se ho zbavíte pomocí tlačítka »Disable«.

Pokud jste si jisti, že název souboru odpovídá špionážnímu nástroji, můžete pro jeho vymazání rovnou použít tlačítko »Remove«. Ve stejném okně najdete uhlazenější variantu Task manageru – Currently Running Programs. Ještě lepším nástrojem na odhalení špionážních utilit je volba „Network Connected Programs", která ukazuje otevřené porty a programy, které mají tuto situaci „na svědomí". Zde je elegantním řešením zablokování komunikace pomocí tlačítka »Block Incoming Connections«.

Pokud můžete na svůj počítač instalovat software, je pro vás ideálním řešením nástroj Process Explorer (**http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx**). Tento nástroj také zobrazuje běžící procesy, nabízí o nich ale mnohem více informací. Většina čmuchalů se snaží své procesy skrýt, Process Explorer je však pro ně obvykle příliš velkým sous-

ŠPIONÁŽNÍ NÁSTROJE LZE ODHALIT

Mnoho špionážních programů lze odhalit pomocí klávesových zkratek, nebo souborů či složek na disku.

Jméno programu	Jak ho odhalit
007 Starr	Start | Run | STARRCMD
Boss Everyware	Soubory BECONFIG.EXE, BEWREP.EXE a RMBEW.EXE v počítači
eBlaster	Soubor URLMKPL.DLL v počítači
Insight	Soubor ISGTCBHO.DLL v počítači
Orvell Monitoring	Klávesová zkratka [Ctrl]+[Shift]+[Alt]+[O]
Silent Watch	Soubory BORLNDMM.DLL, SVCOMSVC.DLL a SVCOMSC.EXE v počítači
Spector Pro	Soubory SHMSWNMP.DLL a SHMSWNRC.DLL v počítači
WinWhatWhere	Složka C:\Windows\System\OLBE v PC

tem. Další výhodou je to, že někteří výrobci špionážních nástrojů vzdali pokusy o skrytí procesů, snaží se pouze používat „nenápadné názvy". Pokud si nejste jisti, komu patří procesy „Explorer.exe" nebo „Window.exe", jediným kliknutím v Process Exploreru je pomocí Googlu prověříte. To vám umožní rychlou a správnou reakci na nalezené „problémy".

Navzdory sledování: Anonymní surfování

Většina společností přímo nemonitoruje „internetovou činnost" každého počítače, ale pouze vnitřní proxy, která však dokáže ukázat, kdo kde surfoval, případně co stahoval. My pro vás máme softwarový tip, který tomu zabrání: JAP – klient An.On projektu univerzity v Regensburgu a Technické univerzity v Drážďanech. Zatímco obvykle je přenos dat uskutečněn přes jeden přístupový uzel, JAP rozdělí data na stovky malých částí a ty pošle v zakódované formě. An.On používá k anonymizaci nejméně tři servery jako mix proxy – počítače, které operátoři JAP klasifikují jako důvěryhodné. Každý mix používá komplikovanou proceduru k míchání dat. A protože proxy operátoři nejsou spolu propojeni, nelze zjistit, kdo jaká data požaduje...

Více se dozvíte v článku na našem webu, kde najdete i další zajímavé informace. Bezpečné surfování vyžaduje určitá nastavení. Nejdříve si z našeho DVD nainstalujte JAP, který vyžaduje pouze Java Runtime (je také na DVD). V tomto nástroji si nejprve musíte zvolit anonymizační servery. V sekci Service zvolte jako „free mix cascade" položku »CCC Kaskade«, což je vhodná volba pro většinu případů. Tímto způsobem můžete přechytračit zvědavost vašeho nadřízeného.

AUTOR@CHIP.CZ