Ochrana přes internet

Internet většině z nás přináší nejen neuvěřitelné množství informací a rozsáhlé možnosti zábavy, ale také pořádné bolesti hlavy, když dojde řeč na bezpečnost. My vám však internet představíme jako vašeho ochránce... *Petr Kratochvíl*

O přínosu internetu z hlediska zábavy není potřeba většinu uživatelů přesvědčovat – každý z nás si čas od času zahraje nějakou tu hru, zhlédne úsměvné video nebo si alespoň přečte třeba vtip. O tom, že na internetu číhá na uživatele i spousta nebezpečí, je už také asi potřeba přesvědčovat jen málokoho – pokud máte to „štěstí“ a chybí vám v tomto ohledu osobní zkušenost, v naší rubrice Bezpečnost najdete dost materiálu ke „studiu“.

Bezpečí z internetu

Jen opravdu málokdo ale ví, že na internetu je možné najít i kompletní „lékárničku“, která váš počítač může dostat zpět do kondice. K dispozici jsou skenery zjišťující přítomnost virů, přítomnost spywaru, nebo dokonce mezery v nastavení firewallu.

Zázraky nečekejte

Je ovšem férové hned v úvodu říci, že od internetových nástrojů nelze očekávat zázraky. Pokud se váš počítač sotva „plazí“, správce úloh úpí pod desítkami procesů a rychlost internetu pomalu klesá na úroveň dial-upu, vaší záchranou bude pravděpodobně pouze reinstalace systému. Shodou okolností se mi těsně před testem dostal do ruky „porouchaný“ notebook mého známého a pravda je, že s téměř 200 viry, 35 spywary a 11 dialery z jeho disku si žádný z internetových nástrojů neporadil. Pomohla až kompletní reinstalace.

Když k této informaci ještě přidáte fakt, že některý malware se vás snaží od internetu „odstřihnout“, musí vám být jasné, že internetové skenery nejsou nástroji „poslední záchrany“. Lze je doporučit především pro řešení menších problémů a mírnějších forem „nákaz“. Ty ale zvládají téměř dokonale.

Nedůvěřujte

Druhou důležitou informací, kterou by měl každý zájemce o „bezpečnost z internetu zdarma“ znát, je míra rizika. Technologie, kterou současné antimalwarové skenery používají (viz rámeček), jim umožňuje téměř neomezený přístup na váš disk. Doporučujeme tedy používat pouze nástroje z důvěryhodných zdrojů a od důvěryhodných firem. Použití „báječného skenu zdarma“ ze stránky s tapetami na plochu přináší stejné riziko jako svěření kufru za účelem pohlídání nemytému individuu z hlavního nádraží. Můžete být příjemně překvapeni, ale za to riziko to nestojí.

Další riziko se skrývá v „překlepech“. Na adrese **housecall.trndmicro.com** nenajdete populární skener od firmy Trendmicro a snaha odstranit spyware pomocí stránky **http://kasperky.com** (místo Kaspersky.com) také nemusí být nejlepším nápadem. V oblasti bezpečnosti se trocha pozornosti rozhodně vyplatí… →

Technologie

V současné době se k on-line skenování používají především dvě technologie – Java a ActiveX. Je zbytečné rozebírat podrobnosti, důležitý je pouze jejich důsledek: pokud je použita Java, lze skener spustit v kterémkoliv browseru. Použití ActiveX omezuje aktivity skeneru pouze na Internet Explorer (a produkty využívající jeho jádro). Pravdou sice je, že existují zásuvné ActiveX moduly i pro Firefox, nejde však o příliš šťastné řešení.

Obě technologie mají své klady i zápory, a nelze tak jednoznačně doporučit pouze jednu z nich. Důležité je ale zdůraznit, že ActiveX představuje relativně velké bezpečnostní riziko (lze ho snadno zneužít k zákeřné instalaci malwaru). U skenerů využívajících Javu zase může docházet k problémům při použití různých verzí. K tomu pravděpodobně došlo i při testování skeneru TrendMicro, který se „zasekl“ a odmítal jakoukoliv spolupráci. Já osobně používám na surfování Firefox, ale při on-line skenu preferuji ActiveX moduly do Internet Explorer.

PROBLÉMY: U nástroje od firmy TrendMicro nám Java dělala problémy...

NEZVLÁDNE: S takovýmto zamořením si on-line nástroje pravděpodobně neporadí...

PRAKTICKÝ: Přehledné výsledky hledání nástroje od firmy BitDefender.

→ Prevence

Pro většinu z nás (včetně mě) je slovo prevence jen zajímavým výrazem ze slovníku, protože heslo „Problémy se řeší, když přijdou“ je až příliš lákavé. Přesto si však pojďme trochu zateoretizovat, jak by šlo většině problémů předejít a co by nám mohlo usnadnit pozdější řešení problémů…

Poznej svůj počítač

Chvíli, kdy dostanete chřipku, poznáte spolehlivě – bolesti kloubů, teplota nebo kašel jsou totiž radikálně odlišné od „provozních vlastností“ vašeho těla. Na podobném principu by měla fungovat i předběžná kontrola vašeho počítače. Pokud víte, jak počítač funguje v „bezproblémovém“ stavu, bude pro vás snadnější odhalit potenciální „nemoc“. Jedním z důležitých ukazatelů „zdraví“ jsou spuštěné procesy. Ve chvíli, kdy na vašem domácím počítači běží více než 50 procesů, nebude zřejmě něco v pořádku. Zde je také důležité poznamenat, že se nevyplatí spoléhat se na standardní nástroj v podobě Správce úloh (skrývající se pod zkratkou CTRL+ALT+DEL). Nejenže se některé viry naučily před ním skrývat, ale tento produkt nevyniká ani přehledností. Lepší je použít Software Explorer z programu Windows Defender, nebo v ideálním případě nástroj Process Explorer. O kvalitách tohoto nástroje (původně od SisInternals) svědčí i to, že ho v současnosti můžete najít i na stránkách Microsoftu…

Kdo je kdo

Nyní už víte, co vám brzdí počítač, ale absolutně netušíte, zda je to dobře, či špatně. Ano, názvy procesů skutečně nepatří k nejpřehlednějším a jen zlomek uživatelů může tušit, co se třeba skrývá pod procesem Nvsvc32.exe. Řešení ale není obtížné: na webu **www.processlibrary.com** najdete podrobné informace o většině procesů skrytých ve Windows, jsou tu i důležité údaje o „dll souborech“. Pomocí této služby tak můžete zjistit, že výše zmiňovaný soubor je „NVIDIA Driver Helper Service“, a pokud máte grafickou kartu od nVidie, nemusíte se ničeho bát. Na výše uvedené stránce najdete i process scanner, který by měl méně zkušeným nebo líněji jedincům podstatně ulehčit práci s kontrolou procesů.

Podobné služby s informacemi o procesech a souborech z Windows najdete i na dalších webech. Doporučit lze například **www.liutilities.com/products/wintaskspro/processlibrary** nebo **www.file.net/process/index.html**.

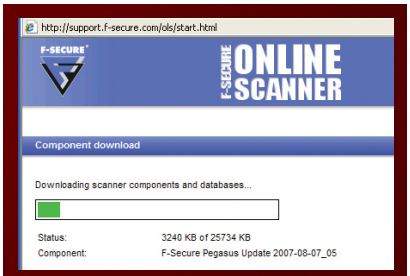
Bezpečný štít

Jedním z nejdůležitějších obranných nástrojů každého surfaře je firewall. Vzhledem k tomu, že jich je celá řada k dispozici zdarma, není problémem jeho pořízení, ale spíše nastavení. Internet vám však „pomůže“ i s touto drobností. Nejen že na něm najdete celou řadu webů s radami „jak nakonfigurovat“, ale také je zde celá řada stránek nabízejících kontrolu „zvenku“. Například na **www.hackerwatch.org/probe** najdete jak kontrolu nastavení firewallu, tak i několik dalších externích testů. Podobné testy najdete i na **www.auditmypc.com/firewall-test.asp**, kde je doplňuje celá řada nadstavbových služeb (od měření rychlosti a zjišťování IP adresy až po test blokování vyskakovacích oken). České varianty testů najdete například na adresách **http://test.bezpecnosti.cz/index.php** nebo **www.paranoia.cz/test/start**.

O stavu bezpečnosti operačního systému se můžete přesvědčit i pomocí nástroje od Microsoftu. Jeho nástroj Microsoft Baseline Security Analyzer (**www.microsoft.com/technet/security/tools/mbsahome.mspx**) je sice určen zkušenějším uživatelům, ale jeho přínos ocení i ti méně zkušení.

Surfuj bezpečně

Poslední (a nejdůležitější) obrannou linií je „lidský faktor“. Sebedokonalejší soft- →



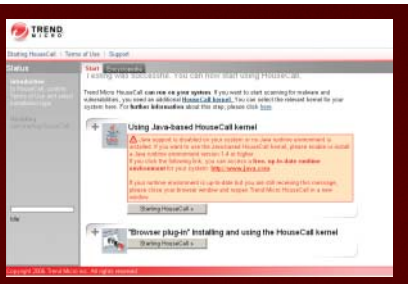
F-SECURE: 26 MB není zrovna ideální velikost pro rychlé použití...

F-SECURE: Hledání virů i rootkitů v popisu práce...

→ warové vybavení se stává zbytečnou haldou nul a jedniček, pokud uživatel nezná základní bezpečnostní pravidla. O rizicích souvisejících s návštěvou jednoznačně rizikových stránek (porno, cracky, warez) je asi zbytečné psát, ale nebezpečí se stále častěji skrývá i na zdánlivě nevinných serverech. O problémech s animovanými kurzory už jste asi slyšeli, ale na spyware můžete narazit například i tehdy, pokud hledáte vyzvánění na mobil, tapety na plochu nebo informace o celebritách. Základním obranným prvkem by mělo být použití bezpečnějšího browseru (Firefox, Opera…), který při vypnutí potenciálních rizik (Java a spol.) zajišťuje slušnou bezpečnost. Důležitým prvkem je zde i obezřetnost – některé nabídky „zdarma" vás ve finále mohou přijít pěkně draho. Rozhodně nedoporučujeme používat nabízené stahovače. Metoda „Tento skvělý soubor si můžete stáhnout, jen když použijete náš stahovač" je jedním z nejpoužívanějších způsobů infiltrace počítače malwarem.

Počítač v ohrožení

Na vašem počítači jsou nejnovější verze antivirů a antimalwarových nástrojů, váš firewall je podezřívavý jak žárlivá ženská a svá Windows záplatujete s železnou pravidelností. Přesto tam je. Nevíte sice ani co, ani kde, ale drobné náznaky vám napovídají, že v systému není něco v pořádku.



FIREFOX I IE: Jediný nástroj od firmy Trend Micro nabízel volbu technologie.

MICROSOFT: Jednoduchý skener především pro začátečníky...

On-line skenery

Prvním nástrojem, který byste měli v tomto případě nasadit, je on-line skener. Jde obvykle o doplněk browseru, který si po stažení aktuálních malwarových řetězců poradí i s nejnovějšími škůdci. Na internetu najdete těchto nástrojů desítky, ale jak jsme se již zmiňovali, doporučujeme používat jen ty důvěryhodné.

Trend Micro

První z testovaných skenerů nabízí na svých stránkách firma Trend Micro. Na adrese **http://housecall.trendmicro.com** najdete stránky, které nabízejí obě technologie on-line skenu (lze tedy použít jak IE, tak Firefox). Nám se ale verzi využívající Javu nepodařilo na testovacím počítači zprovoznit, proto jsme použili kombinaci IE + ActiveX. Samotný sken byl až příliš jednoduchý, chybělo například i tlačítko pro zastavení nebo pozastavení skenu. Jediným projevem „práce" je hlášení Scanning files and folders…

Bitdefender

Jestliže nástroj od firmy Trend Micro charakterizovala až přehnaná jednoduchost, nástroj Bitdefender lze popsat slovem „praktičnost". Ačkoliv Bitdefender využívá pouze Internet Explorer, jeho jednoduché rozhraní ho přímo předurčuje k použití na počítačích začátečníků. Ti by tedy měli zamířit přímo na adresu **www.bitdefender.com/scan8/ie.html**.

Kaspersky

Také tento nástroj od firmy Kaspersky zvolil pro on-line skener technologii ActiveX. Nelíbil se nám delší „startovací čas" nástroje, ale poté jsme byli už jen příjemně překvapeni. Rozsáhlé možnosti skenu (paměť, kritická místa na disku, poštovní schránka…) potěší i profesionály – není nutné zdržovat se prohlížením celého disku. Mírně zklamáni snad mohou být uživatelé sítí, kteří budou postrádat volbu „zkontrolovat pevné disky", protože volba „Tento počítač" spustí i kontrolu namapovaných síťových disků. V každém případě lze ale nástroj na **www.kaspersky.com/virusscanner** doporučit...

Microsoft

On-line skener od Microsoftu pochopitelně využívá technologii ActiveX, s Firefoxem tedy na adrese **http://safety.live.com/site/en-us/default.htm** nepochodíte...

Tento web lze doporučit především uživatelům ovládajícím angličtinu, jinak budete překvapeni, „co vlastně nástroj zkoumá". Ten se totiž na nic nezeptá a rovnou zkontroluje celý počítač – kromě virů a spywaru by měl odhalit i chyby v registrech. Až doposud měli k tomuto nástroji přístup pouze uživatelé z USA, nyní si ho můžete vyzkoušet odkudkoliv…

F-Secure

Stejně jako u většiny nástrojů i zde je využita technologie ActiveX a zabrouzdat sem musíte s Internet Explorerem. Hned v úvodu nám ale vyrazil dech objem stažených dat – 26 MB může být v případě pomalejší linky nepříjemný problém. Na druhou stranu –nástroj provedl nejdůkladnější kontrolu počítače a podle informací v nápovědě by měl detekovat i rootkity.

Najdete ho na **http://support.f-secure.com/enu/home/ols.shtml**. →

Rootkit

Ke klasickým hrozbám jako jsou viry a spyware se poměrně nedávno přidala další, mnohem nebezpečnější - rootkit. Na „unixové platformě" je tato hrozba známa už delší dobu, ale ve Windows se jí mediální pozornosti dostalo až nedávno. Zlomem byl i „první komerční rootkit", kterým firma Sony chtěla chránit svá CD proti nelegálním kopírování.

Na rozdíl od spywaru nebo virů je zde „problém" mnohem větší. Rootkit totiž není nic jiného než software, který dokáže skrýt téměř jakékoliv objekty (procesy, soubory...) v systému. Spyware skrytý pomocí kvalitního rootkitu je tak prakticky neodhalitelný a to samé lze říci o samotném rootkitu. Ideální způsob detekce je boot systému z důvěryhodného média a pokus o nalezení stop, které rootkit může zanechávat ve „vypnutém stavu". Přesto existují nástroje, které se pokoušejí najít rootkit i „za běhu" potenciálně napadeného systému. Na výběr jich je celá řada, tyto si můžete vyzkoušet zdarma:

- RootkitRevealer **www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx**
- Blacklight **www.f-secure.com/blacklight**
- PatchFinder2 **www.rootkit.com/project.php?id=15**

Jakou možnost vybrat?

Každá technologie má své výhody i nevýhody a toto pravidlo platí i pro on-line skenery.

On-line skenery	Klasické antimalwarové programy
Dostupnost: Můžete je využít, ať jste kdekoliv. **Variabilita:** Široká nabídka zaručuje, že si vybere každý. **Zdarma:** Tak širokou nabídku produktů „zdarma" jinde nenajdete... **Aktuálnost:** Nástroj vždy pracuje s nejnovějšími signaturami.	**Robustní:** Bez problémů si poradí i s větším „zamořením". **Ochránci:** Obvykle nabízejí i ochranu v reálném čase. **Samostatné:** K jejich použití nepotřebujete browser.
Omezení: Vyžaduje funkční browser i připojení k internetu. **Slabé:** Neporadí si s masivním zamořením počítače. **Dočasné:** Nabízejí jen jednorázovou pomoc.	**Nutné vybírat:** Na počítači jich nemůžete mít moc, aktivní může být dokonce jen jeden. **Aktualizace:** Nutná neustálá aktualizace, bez ní je použitelnost omezená... **Cena:** Kvalitní produkty nejsou nejlevnější...

→ Grisoft Ewido

Nástroj od Grisoftu s vámi bohužel nekomunikuje česky, ale pouze anglicky nebo německy. Také využívá technologii ActiveX a nabízí volbu kontroly vybraných sekcí (například paměti, registrů nebo pevného disku). I tento nástroj charakterizuje jednoduchost a přehlednost. Vyzkoušet si ho můžete na webu **www.ewido.net/en/onlinescan**.

Eset

Jediný zástupce „česky komunikujících" skenerů též pracuje s technologií ActiveX a bez Internet Exploreru si zde příliš „nepomůžete". Po úvodní inicializaci pravděpodobně většinu uživatelů překvapí „inovativní" počítačové názvosloví. Zde totiž nehledáte viry, malware, spyware nebo rootkity, ale můžete „Hledat nechtěné aplikace" nebo „Odstranit nalezené infiltrace". Co tím chtěli autoři naznačit se neodvažujeme tipovat a raději zaškrtáváme obě možnosti. I přes tuto drobnost lze tento nástroj z webu **www.eset.cz/online-skener** doporučit.

Zkuste to jinak

Několikrát zmiňovanou výhodou on-line skenerů je také možnost použití více nástrojů. Jestliže jeden nástroj nic nenajde, není problém po pár kliknutích vyzkoušet konkurenční nástroj. Nic není ztraceno ani tehdy, pokud se nepodaří skeneru nalezenou „infekci" odstranit. Když víte, jaký škůdce se ve vašem systému skrývá, stačí jen použít jednorázový „čistič". Ty najdete na téměř každém webu antivirové firmy. Doporučit lze například nástroje od Esetu. Jinou efektivní metodou je použití produktu Avast virus cleaner, který lze přirovnat k širokospektrému antibiotiku. Tento nástroj, jenž najdete na adrese **www.avast.cz/cze/avast-virus-cleaner.html**, totiž dokáže snadno odstranit celou řadu nejběžnějších škůdců…

Kontrola souborů

Čas od času se vám „do ruky" dostane podezřelý soubor. Ať už jde o přílohu mailu, „dárek" na USB disku nebo aplikaci staženou z internetu, je zbytečné kvůli němu kontrolovat celý systém. Existují totiž on-line služby, které dokáží libovolný soubor zkontrolovat na přítomnost nežádoucích „hostů". Mezi nejznámější a nejpoužívanější patří následující weby:

- **http://virusscan.jotti.org/**
- **www.eset.cz/online-skener**
- **http://onlinescan.avast.com/index_cze.php**
- **www.kaspersky.com/scanforvirus**

Co doporučit?

Z on-line skenerů nás ani jeden nezaujal natolik, abychom ho prohlásili za jasnou jedničku a doporučili pouze jeho. Naopak – doporučujeme vám jich vyzkoušet několik, což zvýší procento úspěšnosti odhalení škůdců. Přesto vás ale upozorníme na dva nástroje. Pokud spěcháte, bude nejlepší volbou nástroj od firmy Kaspersky, který nabízí i individuální sken paměti a nejčastěji napadaných míst systému. Uživatelé neovládající ani základy angličtiny by zase měli zaměřit svou pozornost na nástroj od Esetu, který s nimi bude komunikovat česky. *Petr Kratochvíl*