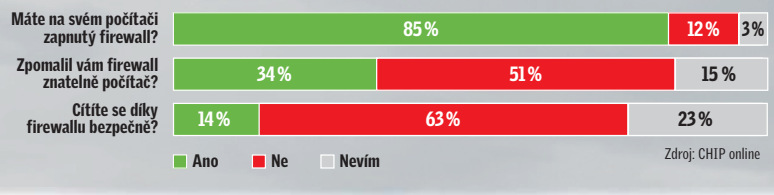
Volnost a bezpečí bez firewallu

Surfovat na internetu bez firewallu je jako lézt po skalách bez jisticího lana: nejste sice ničím omezeni, ale je to nebezpečné. Pokud však znáte ty správné triky, určitě se můžete vyhnout alespoň těm nejhorším internetovým nehodám. *Valentin Pletzer*

Oprávněná nedůvěra v bezpečný firewall?

Téměř každý má na svém počítači firewall, nicméně jen zlomek uživatelů věří v jeho bezpečnostní přínos. Za největší problém při jeho používání označují uživatelé zpomalení počítače...



Zdroj: CHIP online

V tomto článku najdete

Stojíte nad propastí. Máte strach? Není čas. Soustřeďte se na to, co je podstatné: příští krok musí být jistý… Zdá se, že ti, kteří lezou bez jištění, sledují svou cestu téměř bez problémů, dokonce i na strmé skále. Záchrannými lany opovrhují; ta totiž omezují volnost pohybu. Technika a zkušenost zaručují bezpečnost.

Láká vás riziko?

Můžeme to samé aplikovat v internetovém prostředí? Také se jedná o propast: jediné

Na Chip DVD najdete následující nástroje

Spybot Search & Destroy
Kvalitní freewarový nástroj proti malwaru.

Process Monitor
Profesionální analyzátor běžících procesů.

Mozilla Firefox
Alternativní browser pro bezpečnější surfování.

Spamihilator
Jeden z nejlepších programů proti spamu.

Mozilla Thunderbird
Výborný e-mailový klient nabízený zdarma.

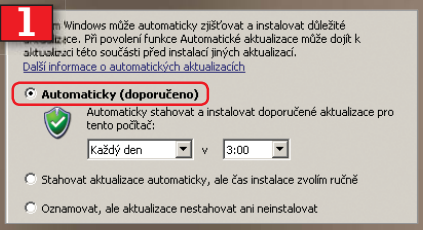
špatné kliknutí a můžete tvrdě dopadnout na stránky se spywarem; stačí si pouze jednou otevřít špatnou e-mailovou přílohu a už můžete ohrozit celou domácí síť či bezpečnostní systém ve firmě.

Pravda je, že z určitého úhlu pohledu nabízejí osobní firewally jen „pochybnou“ bezpečnost. Pochybnou především proto, že už se dávno staly oblíbeným cílem hackerů. Databáze The National Vulnerability (**http://nvd.nist.gov**) již zaznamenala přes 267 „skulin“ v různých firewallech – perfektních vstupů pro útočníky. Navíc firewally omezují bezpečnostní programy: zpomalují systém a „dráždí“ uživatele různými zprávami. Přesto ale nelze firewall jednoznačně odsoudit.

Chip vám představí techniky, které vám umožní pohybovat se po webu relativně bezpečně, i když máte firewall nefunkční nebo když vám chybí úplně. Důležité je zabezpečit tři oblasti: Windows, prohlížeč a e-mailové konto. To vše lze i pomocí bezplatného softwaru nebo se standardními integrovanými nástroji.

Windows mohou být rychlá a bezpečná

1

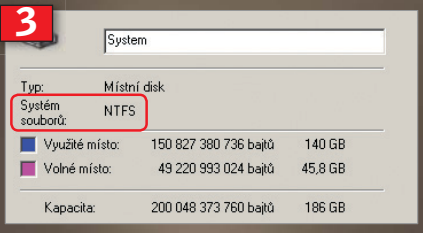


WINDOWS UPDATE: **Nezáplatovaná Windows mají celou řadu „mezer“. Proto stále platí stará a milionkrát opakovaná rada – zapněte si automatický update...**

2

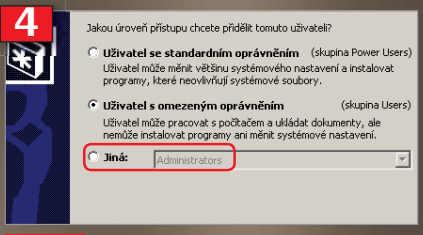
KVALITNÍ ANTIVIR: **Dobrý antivir pomůže i v boji proti malwaru. A pokud najdete na našem DVD výborný antivir AVG zdarma, není nutné dál váhat...**

3



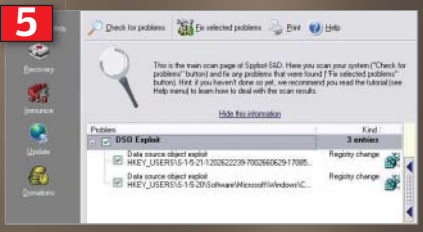
NTFS: **FAT32 byl ve Windows 98 hitem. Ve Windows XP je už brzdou, a to především v oblasti bezpečnosti...**

4



PRÁVA: **Práce s právy administrátora je zbytečné riziko, které většina uživatelů podceňuje.**

5



PROTI SPYWARU: **Kvalitní nástroj specializovaný na boj se spywarem k bezpečnému počítači rozhodně patří.**

Jak ochránit Internet Explorer

Ačkoliv se to zdá divné, ještě stále existují (a kupodivu tvoří významné procento surfařů). Ano, mluvíme o příznivcích Internet Exploreru 6, odmítajících přestoupit na bezpečnější alternativu. Pokud k nim patříte i vy, doporučíme vám minimálně přechod na novější verzi 7 a přidáme pár bezpečnostních triků, které vám alespoň zčásti pomohou udržet škůdce pod kontrolou.

Doporučená bezpečnostní nastavení

Standardní nastavení bezpečnostních parametrů jsou v Internet Exploreru poněkud neuspokojivá. Naše doporučení zní: zpřísněte bezpečnostní opatření před návštěvou rizikové oblasti internetu.

Klikněte v Internet Exploreru na nabídku *Nástroje* | *Nastavení Internetu* a v okně, které se objeví, se přepněte na kartu *Zabezpečení*. Tam zvolte zónu „Internet" a v dolní části okna klikněte na tlačítko *Vlastní úroveň*... Nenechte se zastrašit velkým počtem nabízených položek, my vám poradíme (v tabulce vpravo) optimální nastavení pro nejdůležitější sekce. Zkrátka – rychle deaktivujte vše, co nepotřebujete...

Předcházení problémům

Tak jako námi doporučovaná nastavení umožní spouštět pouze to, co je nutné k bezpečnému surfování, existuje podobná funkce i přímo pro výběr webů: „Servery". Tuto funkci najdete také v okně *Nástroje* | *Nastavení Internetu* | *Zabezpečení*, ale zpřístupní se teprve po volbě zóny *Důvěryhodné servery*. Zde můžete nastavit, které servery považujete za bezpečné a které nebudou procházet sítem vašich bezpečnostních nastavení. Jediným problémem je poněkud špatná přístupnost této funkce – komu by se chtělo proklikávat se mořem příkazů kvůli přidání jednotlivého serveru...

Tento problém však řeší rozšíření jménem „IE5 Power Tweaks Web Accessories" (**www.microsoft.com/windows/ie/ie6/previous/webaccess/pwrtwks.mspx**). I když byl tento doplněk vytvořen pro Internet Explorer 5, spolehlivě funguje i ve verzi 7. Po jeho nainstalování se objeví přímo v nabídce nástroje příkaz „Add to Trusted zone", který vám přidávání bezpečných serverů zjednoduší.

OPEVNĚNÍ WINDOWS

Jak zabránit útočníkům v napadení systému

Nejlepší vstupenkou pro hackery je ve Windows konto administrátora. To proto, že po typické instalaci Windows XP existuje jedno konto, které je vybaveno právy administrátora – s bezproblémovým přístupem do celého systému! Obtíže nastanou, jakmile uživatel s právy administrátora spustí Outlook Express a tento e-mailový klient otevře mail zamořený virem. Tento vir může totiž poté provádět přesně to, co může provádět administrátor. Abyste předešli takové nepříjemnosti, doporučujeme surfovat s obyčejnými „uživatelskými" právy . Dále doporučujeme provést následující kroky:

Bezpečnostní nastavení	Deaktivovat
.NET Framework	
Dokumenty XPS	✖
Formát Loose XAML	✖
XAML – aplikace prohlížeče	✖
Ovládací prvky ActiveX a moduly plug-in	
Chování skriptů a binárních souborů	✖
Ovládací prvky ActiveX skriptu byly označeny jako bezpečné pro skriptování	✖
Spouštět ovládací prvky ActiveX a moduly plug-in	✖
Komponenty využívající technologii .NET Framework	
Spustit komponenty pomocí technologie Authenticode	✖
Povolit nastavení rozhraní .NET Framework	✖
Různé	
Instalace součástí pracovní plochy	✖
Odesílat nezašifrovaná formulářová data	✖
Povolit parametr META REFRESH	✖
Povolit webovým stránkám použití omezených protokolů pro aktivní obsah	✖
Přetahování nebo kopírování a vkládání souborů	✖
Softwarové oprávnění kanálu	Vysoké zabezpečení
Spouštění aplikací a nedůvěryhodných souborů	✖
Spouštění programů a souborů v sekci IFRAME	✖
Trvalost uživatelských dat	✖
Webové servery obsahu ve více omezené zóně mohou přejít do této zóny	✖
Zobrazit smíšený obsah	✖
Skriptování	
Aktivní skriptování	✖
Povolit přístup pro programování do schránky	✖
Skriptování appletů v jazyce Java	✖
Stažení	
Stažení písma	✖

1 Nejdříve ze všeho si aktivujte automatické záplatování ve Windows Update. Pokud je váš operační systém aktualizovaný, značně to redukuje šance k zamoření. Také aktivujte automatický update pro všechny další používané aplikace: díry v Quicktimu, Photoshopu nebo Flashi jsou pro hackery v současné době horkým favoritem.

2 Dalším krokem by měla být instalace antiviru. Dobrý antivirový program dokáže identifikovat převážnou část malwaru, a to dokonce i předtím, než je aktivován. Jako doplněk doporučujeme ještě přidat dobrý antispywarový program – například Spybot Search & Destroy.

3 Nakonec zbývá už jen jediné. Abyste předešli snadnému porušení zadaných pravidel, systémová partition musí být naformátována v NTFS. Na rozdíl od FAT32 totiž NTFS podporuje službu Active Directory, která je pro bezpečnost uživatelských účtů důležitá.

Z FAT32 na NTFS

Brečet ale nemusíte ani tehdy, pokud jste si nainstalovali XP v systému FAT32. Naštěstí lze systém změnit i později. Dříve než se do toho pustíte, si však zálohujte všechna důležitá data – pro jistotu. Ačkoliv tato konverze ve většině případů proběhne bez problémů, je lepší se jistit, než později litovat. Po zazálohování si otevřete příkazový řádek v nabídce *Start* | *Programy* | *Příslušenství* a napište:

```
Convert C:/fs:NTFS
```

Pozor: Tento proces trvá několik minut, v závislosti na velikosti disku, který konvertujete.

4 Další krok má smysl pouze tehdy, jestliže jste už svůj systém převedli do NTFS: otevřete *Start* | *Control Panel* | *User Accounts* a vytvořte dalšího uživatele s právy administrátora. Jakmile ho vytvoříte, převeďte svůj účet na „obyčejný s uživatelskými právy". Toto opatření vám poskytne maximální ochranu nejen při surfování.

5 Celá věc má ale jeden háček: některé programy zbytečně (a proti programátorskému kodexu Microsoftu) používají zdroje, které jsou vyhrazeny pro administrátora a systém. To pak může při spouštění s „obyčejnými" uživatelskými právy dělat neplechu. Problém se většinou objeví už během instalace.

Řešení: Uživatelé s omezenými právy spouští instalaci volbou *Spustit jako...*,

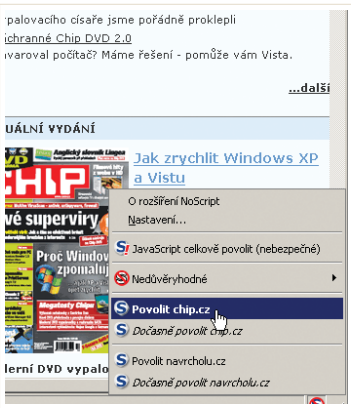
která se objeví v kontextovém menu při kliknutí pravým tlačítkem na soubor. Potom zvolte konto administrátora a pomocí hesla potvrďte akci. Pokud to nefunguje, nainstalujte problematický program přímo z konta administrátora pro všechny uživatele a poté se zase přepněte zpátky do svého „normálního“ konta.

Řešení problémů

Nepomůže-li ani tento postup, máte dvě možnosti. Jednak se vždy můžete přepnout do konta administrátora, budete-li chtít použít problematický program. Vše, co musíte udělat, je vybrat v nabídce *Start | Vypnout…* volbu *Odhlásit uživatele…*

Druhá možnost je do určité míry určena pro profesionály. Program „Sysinternals Process Monitor“ od Microsoftu je zdarma a je k dispozici na **www.microsoft.com/technet/sysinternals/utilities/processmonitor.mspx**. Může vám pomoci při hledání zdrojů, na kterých program závisí.

A jak na to? Spusťte nástroj pomocí příkazu *Spustit jako…* s právy administrátora. Pak otevřete program, který dělá problémy. Jakmile se chyba objeví, přepněte se zpátky na monitor procesů a zastavte protokol pomocí klávesové kombinace [Ctrl] + [E]. Abyste našli problematické procesy, stiskněte klávesovou kombinaci [Ctrl] + [L] a filtr nastavte pomocí výrazů „Result, contains, Access Denied“. Filtr potvrďte kliknutím na *Add* a *OK*. Program nyní znázorní pouze hledané zamítnuté přístupy (rejected accesses). Kliknutím pravým tlačítkem na nalezenou položku a poté na *Jump to* se přímo přepnete na indexy či položky v registrech, jež ukazují, ve kterých složkách či souborech se chyba objevila.



NO SCRIPTS: **Plug-in NoScript do Firefoxu dokáže zneškodnit nebezpečné skripty.**

Pokud se jedná o složku, klikněte na ni pravým tlačítkem, otevřete *Vlastnosti* a zvolte záložku *Security*. V nabídce „Groups or user names“ zvolte své uživatelské jméno a poté zkontrolujte sekci „Authorization for“ – především položky „Read“ a „Write“. Které položky byly „problematické“, to si můžete vyhledat v procesovém monitoru ve sloupci „Operations“.

Podobně funguje také přidělení práv v souborech.

ZABEZPEČENÍ BROWSERU

Chybné akce na nebezpečných stránkách

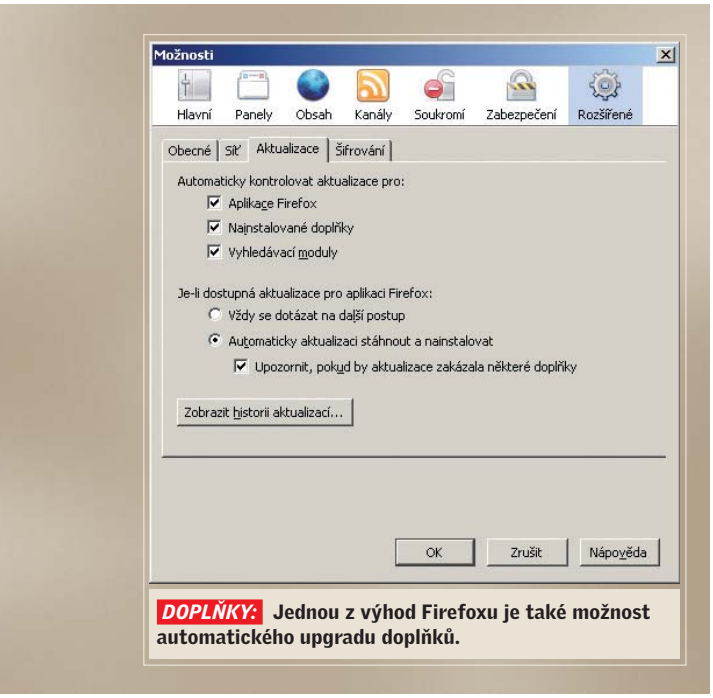
Jeden špatný pohyb na internetu a systém je infiltrován. Internetové „bezpečnostní“ seznamy ukazují, že internetová mafie se spoléhá hlavně na Internet Explorer a na jeho „plug-iny“. Zde se totiž nachází spousta bezpečnostních děr.

Jak to funguje

Pozadí: Oběť je nejprve nalákána (převážně pomocí e-mailu) na zdánlivě neškodný web, který ale obsahuje nebezpečnou stránku. Na ní JavaScript nejdříve otestuje systémovou konfiguraci a poté spustí vhodný útok. Další postup je pak ve všech případech stejný. Oběť „obdrží“ malý stahovač, který poté nahraje vybraného škůdce. Komponenta stahovače není na první pohled nijak problematická, proto je její identifikace pro antivirové produkty komplikovaná. Jakmile je jednou stahovač aktivní, nejprve vypne všechny bezpečnostní produkty. Škůdce, který je stažen později, ve většině případů pátrá po důležitých datech a heslech.

Řešení: Je to sice „stará“ rada, ale má svůj smysl: zapomeňte na Internet Explorer a přejděte na Firefox nebo Operu. Na Chip DVD najdete jejich nejnovější verze. Ani jeden ze zmiňovaných prohlížečů není bez chyby, ale především u Firefoxu platí, že jakmile internetová komunita najde nějaké díry, během pár dnů jsou obvykle utěsněny.

Kromě toho existují i plug-iny, které učiní Firefox ještě bezpečnějším. Jedná se například o praktický NoScript, který vyřeší jeden velký problém. Základnou většiny útoků je totiž JavaScript. Jeho úplné vypnutí však není řešením, protože spousta dobrých webů ho používá, aby byly jejich webové stránky pohodlnější – klíčovým slovem je tu termín „Web 2.0“. A zde přichází ke slovu NoScript. Přestože



DOPLŇKY: **Jednou z výhod Firefoxu je také možnost automatického upgradu doplňků.**

celkově blokuje skripty, je-li to zapotřebí, nabízí jednoduchou možnost, jak JavaScript znovu aktivovat pro spolehlivé stránky.

Jak na skripty

Jakmile je NoScript aktivní, prohlížeč zobrazí jeho ikonu v pravém spodním rohu. Ve standardním nastavení se ve spodní liště za každý blokovaný skript objeví poznámka. Kliknutím na položku *Settings* lze povolit skripty z určitých domén dočasně, vždy nebo nikdy. Jestliže například surfujete na novém webu Chip.cz, asi budete chtít povolit všechny skripty, které jsou na serveru aktivní. Stačí jen zvolit možnost *Allow chip.cz* a vše bude fungovat…

FILTROVÁNÍ E-MAILŮ

Zákaz vstupu pro spam a phishingové maily

Podle různých studií tvoří až 95 procent všech e-mailů zasílaných po celém světě spam nebo phishingové maily. Problémem je, že bývá stále obtížnější odlišit dobré maily od těch špatných. Triky typu „šifrování zpráv se soubory PDF“ rapidně zhoršují účinek antispamových filtrů. Navíc relativně velké soubory drasticky zvyšují internetový provoz a snadno zaplňují i poměrně velké e-mailové schránky. Řešení tohoto problému však může být relativně jednoduché:

1 Vybavte svůj systém kvalitním spamovým filtrem. Doporučujeme freewarový Spamihilator, protože nástroj je transparentní v době připojování e-mailového klienta k serveru. Jeho další výhodou je možnost použití v celé řadě e-mailových klientů. A jak na to? Nejprve zavřete svůj e-mailový program a spusťte instalaci Spamihilatoru. Během ní vás průvodce provede celým instalačním procesem a také vám nabídne doporučeníhodná nastavení. Ke konci instalace se občas objeví žádost, abyste si zvolili svůj e-mailový program. Oblíbení klienti jako Outlook Express či Thunderbird jsou Spamihilatorem rozpoznány a nakonfigurovány automaticky.

2 Proti nejnovějším variantám spamu využívajícího PDF se můžete bránit pomocí užitečných plug-inů. Doporučujeme například „Empty-Mail-Plugin“, který odfiltruje každý prázdný či extrémně malý textový e-mail.

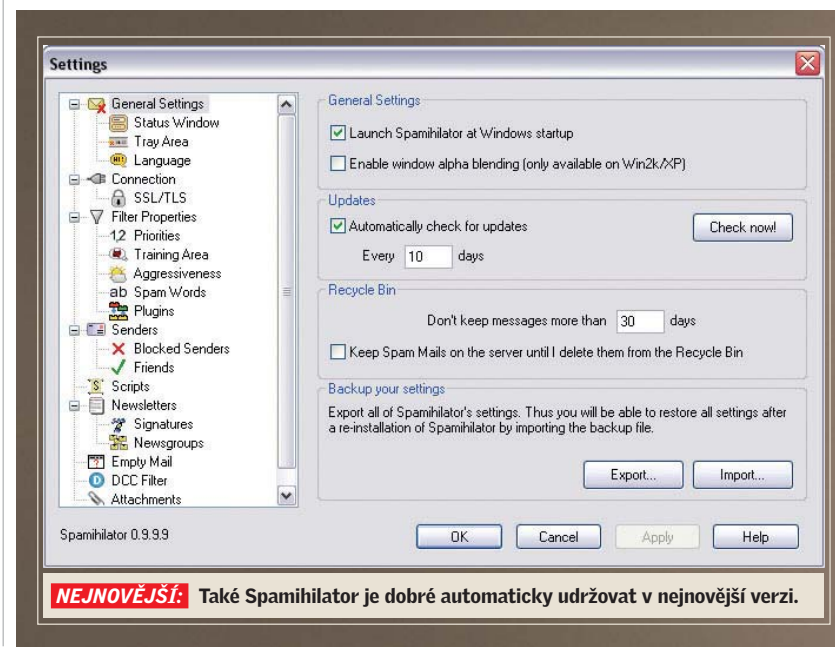
Abyste si filtr nainstalovali, musíte nejprve kliknout pravým tlačítkem myši na ikonu Spamihilatoru, která se nachází dole v liště „systray“, a v nabídce, která se objeví zvolte *Settings*. V následujícím okně se přepněte do karty *Filter Properties | Plugin* a klikněte na tlačítko *Other Plugins…* Nyní označte položku „Empty Mail Filter“ a poté klikněte na tlačítko *Install*. Plug-in je stažen a nainstalován automaticky. V nastavení Spamihilatoru nyní najdete novou volbu „Empty Mail“, která umožní jemné doladění plug-inu.

Pokud jste si například jisti, že neobdržíte žádný „normální“ e-mail s přílohou ve formátu PDF, ještě vhodnější bude „Attachment-Extension Filter“. Tento plug-in může být nastaven tak, že všechny maily s přílohou PDF jsou klasifikovány jako spam. Tento plug-in je přímo součástí paketu Spamihilatoru a najdete ho pod *Settings | Attachment*.

3 Nastavte si svého e-mailového klienta tak, aby se v případě mailu ve formátu HTML nezobrazovaly automaticky obrázky načítané z internetu (často jsou také označovány jako externally hosted images). Tímto způsobem si spammer kontroluje, zda je e-mail používán.

Na závěr jen dodáme, že i zde doporučujeme „alternativní“ program, a to Thunderbird. E-mailový program od výrobců Firefoxu je pohodlný a má bezpečnostní výhody. Útoky na Microsoft Outlook a Outlook Express jsou totiž stejně časté jako na Internet Explorer. Obecně lze říci, že čím méně rozšířený produkt používáte, tím menší je riziko hackerského útoku.

Valentin Pletzer



NEJNOVĚJŠÍ: **Také Spamihilator je dobré automaticky udržovat v nejnovější verzi.**