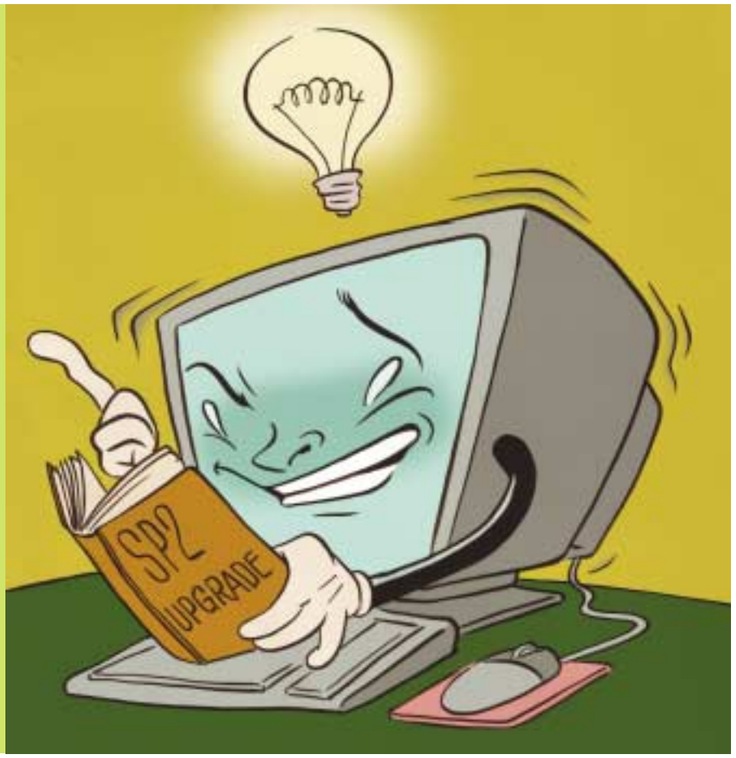
Již před časem jsme psali o tom, že mezi hlavní novinky v balíku Service Pack 2 pro operační systém Windows XP patří řada bezpečnostních vylepšení. Tato formulace však představuje nejhrubší zjednodušení, a proto se v následujících odstavcích podrobněji zaměříme na to, jak současné možnosti ochrany vašeho počítače využít. Pokud chcete dobře porozumět některým možnostem nastavení, kolem nichž jste prozatím jen procházeli se zatajeným dechem, je tento článek určen přesně pro vás.



Maximální bezpečnost

Windows XP SP2 je zaměřen na ochranu PC

PATRIK MALINA

Společnost Microsoft uvedla zásadní opravný a „vylepšovací" balík pro klientská Windows XP již ve druhé polovině minulého roku a mohlo by se tedy zdát, že téma není až tak aktuální.

Ve skutečnosti bylo do tohoto systémového upgradu zařazeno tolik změn, že řada uživatelů, třeba z neznalosti či obav z možných následků, jejich možností buď dosud nevyužívá, nebo ochranu raději co nejpečlivěji vypíná, aby systém náhodou „nepřestal chodit". Pokud se chcete blíže zaměřit na podrobnou konfiguraci důležitých bezpečnostních mechanismů, přinášíme vám zde podrobného průvodce, s jehož pomocí uvedené postupy určitě zvládnete.

Firewall je dnes nezbytný

Přestože vám možná řada „dobrých kamarádů" a „zkušených uživatelů" z bezprostředního okolí bude tvrdit pravý opak, smiřte se se skutečností, že bez zapnutého osobního firewallu je dnes přístup k internetu z domácího počítače ryzí hazard, ba co víc, jeho pomalá likvidace. Navíc ani tolik nezáleží na tom, jaký druh internetové konektivity využíváte: značné problémy mohou mít jak majitelé vytáčeného připojení (dial-upu), tak uživatelé modernějších služeb, přičemž samozřejmě platí, že čím je připojení více permanentní a širokopásmové, tím většímu nebezpečí se vystavujete. Pro upřesnění uveďme, že po připojení pomocí běžné ADSL linky vás nějaký pokus o síťový útok s vysokou pravděpodobností potká mezi prvními 15 a 30 minutami a váš další osud může těsně souviset právě s tím, co na vás toto „první oťukání" prozradí.

Komponenta Windows Firewall byla v balíku SP2 značně vylepšena a přepracována, takže dnes představuje opravdu zajímavé řešení. Její konfiguraci můžete v grafickém prostředí zahájit buď pomocí stejnojmenné položky v *Ovládacích panelech,* nebo také nepřímo, přes zcela nové rozhraní *Centra zabezpečení* (*Security Center*, též v *Ovládacích panelech*). **[obr. 1]** Než začnete Windows Firewall konfigurovat, ještě jedno upozornění: pokud máte v systému nasazen jiný produkt tohoto druhu, raději zapínejte jen jeden z nich a ne více zároveň. Výsledné chování by opravdu mohlo být nevyzpytatelné.

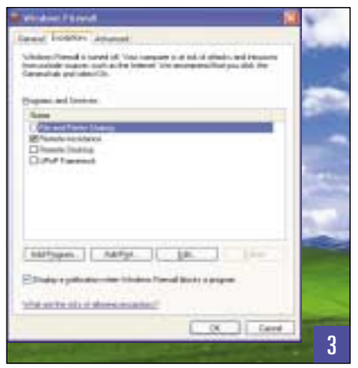
Kromě základních možností – tedy vypnutí a zapnutí firewallu – naleznete na titulní kartě *General* ještě volbu *Don't allow exceptions (Nepovolovat výjimky).* **[obr. 2]** Pro vyjasnění jejího významu si připomeňme, jak v základním režimu firewall pracuje. Prostým zapnutím dosáhnete stavu, kdy odchozí komunikace je propouštěna, tedy vaše požadavky do sítě odcházejí, a opačný směr – příchozí požadavky – jsou považovány za neoprávněné a jako takové jsou blokovány. Tento stav můžete právě ovlivňovat povolením *Výjimek (Exceptions),* díky nimž lze přesně říci, jaký typ komunikace bude v „nebezpečném" směru, tedy z okolní sítě do vašeho počítače, propouštěn. V řadě případů jsou výjimky užitečné, neboť dovolují, abyste mohli třeba sdílet soubory v síti, ale v některých situacích je jejich použití skutečně riskantní: pokud se nacházíte třeba s přenosným počítačem na cestách a jste připojeni do neznámé sítě, dočasně raději výjimky zakažte a pracujte v režimu „ven vše, dovnitř nic".

Pracujete-li v síťovém prostředí, kde jsou výjimky užitečné a ospravedlnitelné, pak se jejich použití nebojte. Na kartě *Exceptions (Výjimky)* najdete předem připravený základní seznam pro běžné služby operačního systému, jež byste mohli potřebovat. Jednou z nich je *Sdílení souborů a tiskáren (File and Print Sharing).* **[obr. 3]** Zvolte ji v případě, že ze sítě okolo vás potřebuje někdo přistupovat na vámi sdílený adresář nebo tiskárnu. Pozor: v jiném případě tuto výjimku nepovolujte, může to být dosti nebezpečné. A nezapomeňte, že pokud navštěvujete sdílené adresáře na jiných počítačích, tuto výjimku nepotřebujete, neboť se jedná o spojení odchozí!

Dalšími službami jsou *Vzdálená pomoc (Remote Assistance)* a *Vzdálená plocha (Remote Desktop),* jež se mohou hodit při vzdáleném přístupu na váš počítač jak vám samotným, tak administrátorům vaší sítě či jiným uživatelům, kteří vám chtějí pomoci. Pokud jste tyto dvě služby nikdy nepoužili a nepotřebujete je, pak pochopitelně výjimku vůbec nezapínejte. Podrobněji o službě Remote Desktop a jejich příbuzných se dočtete v tomto čísle PC WORLDu v rubrice Software, kde také můžete zjistit, zda se vám bude k něčemu hodit. Z dalších služeb pak v přehledu ještě najdete *Universal PnP*, kterou opravdu zapínejte jen v případě, že to z nějakého speciálního důvodu budete potřebovat. Slouží k automatické konfiguraci ve spolupráci s jinými síťovými zařízeními a příliš často na ni asi nenarazíte.

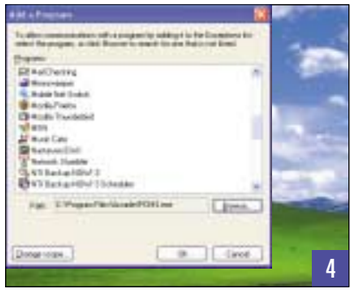
1

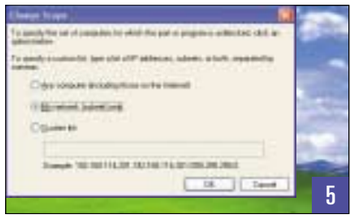

2

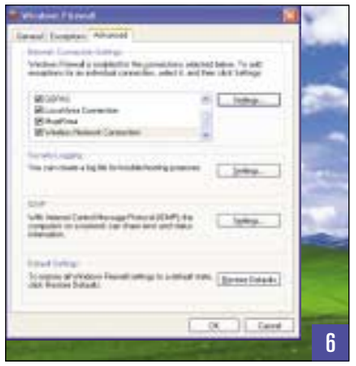

3

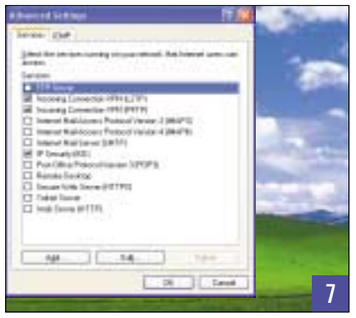
V seznamu pochopitelně chybí specifické služby, o nichž tvůrci netušili, že je můžete potřebovat. Mohou sem patřit třeba aplikace pro internetovou telefonii či třeba hry, provozované po síti, jež potřebují komunikovat směrem „dovnitř". Jejich přidání mezi výjimky zařídíte dvěma způsoby. První možností je přímo otevřít vymezené porty protokolu TCP či UDP, aby žádoucí komunikace mohla na váš počítač protéci zvenčí – nevýhodou je zde to, že ona čísla portů musíte znát, což často znesnadňuje skutečnost, že se mohou průběžně měnit. Výbornou novinkou tedy je, že pomocí tlačítka *Přidat program* lze vybrat přímo aplikaci, které bude naslouchání povoleno. **[obr. 4]** Jde o velmi pružné řešení, neboť sám spuštěný program pak firewallu říká, jaké kanály potřebuje. Při výběru portů či povolených aplikací si všimněte ještě dalšího důležitého tlačítka *Change Scope.* S jeho pomocí přesněji určíte, ze které sítě příchozí požadavky očekáváte. Máte na výběr mezi celým „zbytkem světa", podsítí, v níž se sami nacházíte, nebo přesným seznamem IP adres počítačů a sítí, jimž budete důvěřovat. **[obr. 5]** Než opustíme seznam výjimek, ještě upozorníme pro ujasnění na důležitou skutečnost: tato nastavení povolují příchozí provoz, jenž bude zpracován přímo na vašem počítači a jeho „spotřebitelem" tedy bude služba nebo aplikace na témže stroji. Pokud přes Windows Firewall chcete propustit datové toky, jež budou pokračovat dále do sítě (třeba při sdílení internetové linky) nebo potřebujete další služby, o nichž zde nebyla řeč, musíte použít nastavení na třetí záložce *Advanced*. **[obr. 6]**

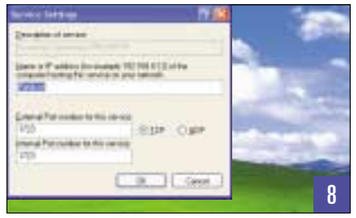
Právě karta tohoto označení přináší velmi důležité a zajímavé novinky. Nejdříve se budeme zabývat její horní částí, kde naleznete seznam momentálně existujících síťových připojení. Právě zde, prostřednictvím označení příslušného síťového rozhraní a následným stiskem tlačítka *Settings*, se vám otevírá možnost dodatečně specifikovat výjimky, jež dovolí otevřít cestu příchozí komunikaci, ale právě a jen ze směru, s nímž pracujete. Na zobrazené kartě najdete opět několik připravených položek pro okamžité použití, mezi nimiž dominují poštovní a webové služby, ale pokud zprovozníte třeba VPN spojení, naleznete zde příslušné protokoly PPTP či L2TP. **[obr. 7]** Pokud jednu z možností označíte a nahlédnete do úprav pomocí tlačítka *Edit*, všim-

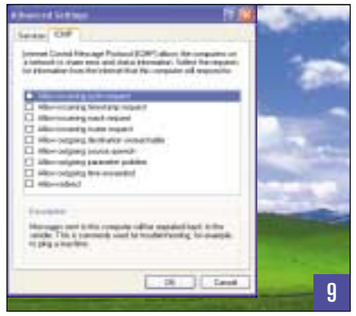

4

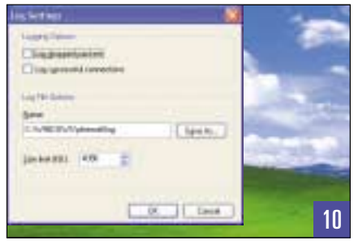

5


6


7


8


9


10


11

něte si, že je možné jako cílový počítač zadat adresu sebe sama (pak bude komunikace ukončena na vašem rozhraní a předána službě ke zpracování), nebo jiný stroj, ukrytý ve vaší síti (v případě sdílení internetové přípojky). **[obr. 8]** Podobně jako u dřívějších *Výjimek* i zde je možné sestavit pomocí volby *Add (Přidat)* vlastní definici protokolu podle čísla portu, na němž budete naslouchat. Než pokročilá nastavení opustíme, ještě nahlédněte na kartu ICMP. **[obr. 9]** Protokol stejného jména slouží primárně k testovacím účelům a může posloužit k užitečnému monitorování sítě, na druhou stranu se může stát rafinovanou zbraní. Právě zde tedy platí, že požadavky z firemní či domácí sítě je možné akceptovat, avšak z veřejného internetu tyto pakety prakticky vždy zahazujeme. Před použitím se opět o protokolu ICMP blíže informujte. Nacházíte-li se však v jednoduché situaci – domácí internet na jediném počítači, pak platí jediné: ICMP domů nesmí!

Po návratu na kartu *Advanced* zde najdete ještě některé zajímavé možnosti. Jednou z nich je logování, tedy pořizování záznamu o činnosti firewallu. Pokud tuto možnost využijete, v první řadě doporučujeme zásadně zvětšit velikost ukládaného logovacího souboru alespoň na několik MB, pro začátek zaznamenávejte pouze zahozené (dropped) pakety, abyste měli představu o marných pokusech proniknout do vaší sítě. **[obr. 10]**

Na kartě *Advanced* ještě najdete globální nastavení pro ICMP zprávy, jež je podobné tomu u jednotlivých síťových rozhraní, a tlačítko pro návrat do výchozí konfigurace. Pokud jste si s nastavením firewallu hodně pohráli, tak jej samozřejmě míjejte velkým obloukem.

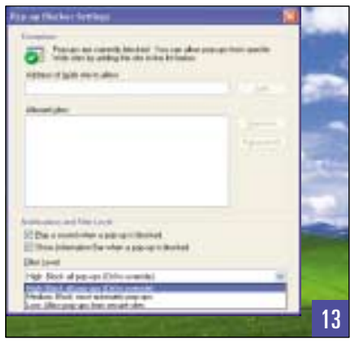
Na závěr uveďme, že pro automatizovanou a pokročilou správu Windows Firewallu lze použít rovněž příkazovou řádku, přesněji konzolovou aplikaci Netsh. Ta zahrnuje sadu příkazů, pro něž najdete nápovědu přímo v *Centru pomoci a nápovědy* nebo v příkazové řádce po zadání *„Netsh firewall ?“*. **[obr. 11]**

Za bezpečné surfování

Vývojáři Windows se samozřejmě nezaměřili jen na zabezpečení sítě pomocí firewallu, neboť je dobře známo, že řadu problémů sebelepší síťová ochrana neřeší. Jednou z typických situací je používání internetového prohlížeče, jež vede často k zavlečení či spuštění škodlivých programů, ačkoliv firewall pracuje, seč mu síly stačí. Právě proto najdeme v prohlížeči některá zajímavá vylepšení, na něž se nyní podíváme.

Velmi zajímavým a důležitým rozhraním je správce zásuvných modulů a podpůrných komponent prohlížeče Internet Explorer. Jeho rozhraní najdeme v prohlížeči v menu *Tools (Nástroje)* jako položku *Manage Add-ons*… **[obr. 12]**


12


13

V otevřeném okně lze poté vyhledat seznamy, mezi nimž můžete přepínat prostřednictvím rolovacího menu v horní části. Ve velkém okně poté objevíte kolekce modulů, jež jsou prohlížečem využívány pravidelně nebo byly použity alespoň jednou. K jejich identifikaci vám může pomoci především jméno samotné součásti a také její vydavatel. Kteroukoliv z položek můžete ve sloupci se jménem označit a poté v dolní části okna dočasně či trvale vypnout. A jak vlastně rozpoznat, co sem patří? V první řadě by zde měly být moduly, u nichž jasně identifikujete výrobce a jste si jisti, že jste jejich instalaci povolili. Pokud si nevíte rady, zkuste podle jména souboru, v němž se modul nachází, dohledat adresář s jeho fyzickým uložením, což vám může osvěžit paměť, zda jste jej instalovali nebo ne. Podezřelé kousky zkuste dočasně zakázat a uvidíte, jak se to projeví.

Další zajímavou novinkou v prohlížeči je blokování vyskakovacích oken, tzv. Pop-up Blocker. **[obr. 13]** Jde o velmi užitečnou funkci, neboť nevyžádaná vyskakovací okna nejen zdržují práci, ale také mohou obsahovat škodlivý kód, jenž počítači dokáže ublížit. Nastavení této komponenty naleznete opět v menu *Tools (Nástroje)* a samotná konfigurace je prostá. Do seznamu povolených stránek lze přidávat položky, určující vámi prověřené zdroje, jejichž pop-up okna jsou důvěryhodná a chcete je používat. V dolní části pak rolovací seznam nabízí možnosti, v jak důsledném režimu budou tato okna filtrována. Nejlepší je nastavit na zkoušku prostřední úroveň a sledovat, jak si prohlížeč poradí s běžným provozem – v případě problémů lze kontrolu zpřísnit a prakticky vše odfiltrovat.

S internetovým prostředím a prohlížečem také souvisí série drobných vylepšení, které se týkají stahování a spouštění souborů. Nově byly přepracovány dialogy, jež jsou zobrazeny při snaze spustit stahovaný soubor z internetu, ale také při otevírání přílohy z e-mailu. Tato důkladnější kontrola umožňuje uživateli důsledněji hlídat, od koho vlastně software, který chce do počítače umístit, pochází. Jde o drobná, ale důležitá vylepšení. **[obr. 14, 15, 16]**


14

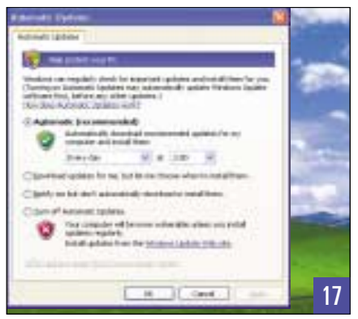

15

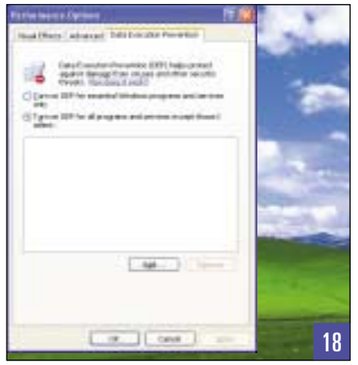

16

Další služby

Řada nových možností, jež přišly se Service Packem 2, není tak dobře viditelná jako výše uvedené příklady. V této části se podíváme na některé další zajímavosti, o nichž byste měli vědět.

Vedle firewallu je dnes již takřka nepostradatelnou službou Automatic Updates (též Windows Update), tedy mechanismus automatizovaného stahování a instalování bezpečnostních oprav operačního systému. **[obr. 17]** Jeho konfiguraci naleznete v *Ovládacích panelech* a systém vám nabízí čtyři úrovně, na nichž služba dokáže pracovat. Ideální je samozřejmě volba plně automatická, jež zajistí stažení i instalaci oprav sama, ale ta nemusí být vždy úplně praktická třeba v domácí síti, kdy byste internetové toky rádi regulovali. Pokud chcete jen řídit čas instalace a zátěž internetové linky vás netrápí, použijte volbu druhou, jež pouze stahuje, ale poté instalaci jen nabídne. Třetí možnost pak vždy jen oznamuje a zbytek je na vás (od stažení po instalaci). Volbu čtvrtou nelze doporučit, neboť alespoň oznamování byste používat měli. Nezapomeňte, že přes neošetřené díry proudí do systémů většina škodlivého kódu, což není propaganda, ale tvrdá realita.


17


18

Mimo jiné i s výskytem bezpečnostních děr souvisí další ochranná funkce operačního systému, nazývaná Data Execution Prevention, tedy prevence spuštění dat (kódu). **[obr. 18]** Protože název zní trošku podivně – různé soubory přece musíme spouštět, abychom počítač mohli používat – je na místě drobné vysvětlení. Tato funkce má za úkol bojovat s podvratnými programy (červy apod.), jež se snaží o provedení nějakých programových instrukcí, ovšem často tím způsobem, že neoprávněně zasahují do oblastí operační paměti, jež byly jasně vymezeny pro jiné, legální aplikace. A právě tato nová komponenta má za úkol takové „přehmaty“ odhalit a zabránit škodlivým programům v útočné činnosti tím, že jim nedovolí zasahovat do nežádoucích paměťových oblastí, kde typicky pracuje operační systém a jeho služby. Cílem je tedy útočný kód izolovat tak, aby nemohl uškodit. Jde především o boj proti chybám, jež jsou známy jako buffer overrun či overflow, tedy „přetečení zásobníku“, jejichž nebezpečnost je často považlivě vysoká. K samotnému nastavení této funkce se dostanete, když na ikoně *Tento počítač* pravým tlačítkem vyberete *Možnosti (Properties)* a na kartě *Advanced* stisknete v horní části v poli *Performance (Výkonnost)* tlačítko pro bližší konfiguraci. Karta *Data Execution Prevention* (jinak též *DEP*) je poměrně skromná: v základní podobě je aktivní volba, chránící důležité služby a aplikace pro samotnou činnost Windows. Případně můžete ochranu zesílit tím, že jí rozšíříte na všechny služby a aplikace, mezi nimiž pak můžete vybrat čestné výjimky. Pokud v tomto případě „přitvrdíte“, může se stát, že kontrolní mechanismus některé jinak potřebné aplikace bude blokován. Pokud se tak stane, přesvědčte se o jejich původu a pak je buď přidejte mezi výjimky, nebo je zkuste instalovat v novějších, korektnějších verzích.

Závěrem

Dlouho připravovaný balík Service Pack 2 pro Windows XP zdaleka nepřinesl pouze vylepšení bezpečnosti a už vůbec ne jenom ta, o nichž jsme mluvili. Novým funkcí byla celá řada, avšak tyto patří k těm nejdůležitějším. Jste-li „správci“ svých počítačů, připojených k internetu, měli byste o nových vymoženostech vědět. K jiným novinkám se třeba dostaneme zase příště. 5 0103/FEL ❑