Nový Service Pack 2 pro Windows XP

Optimální instalace SP2

Microsoft troubí k útoku na viry a hackery. Kromě sbírky oprav chyb obsahuje SP2 řadu nových ochranných mechanismů. Chip se podíval, co přinášejí a jak fungují.

Stalo se toho hodně: Internet Explorer prošel generální revizí, Outlook Express podědil některé rysy od svého velkého bratra Outlooku a Windows Firewall se nyní dá obsluhovat podstatně jednodušeji. Celkově lze říci, že Microsoft svůj dřívější slib - investovat více energie do bezpečnosti Windows - novým balíčkem Service Pack 2 opravdu plní. Nejaktuálnější verzi SP2 (zatím anglickou) najdete na http://www.microsoft.com/ technet/prodtechnol/winxppro/maintain/wi nxpsp2.mspx.

BLOKOVÁNÍ REKLAMNÍCH OKEN

Ankety mluví jasně: Reklamní "pop-upy", které postupem doby zaplavily skoro každou komerční internetovou stránku, návštěvníky webu popuzují. Za znechucené uživatele teď Microsoft prostřednictvím SP2 láme kopí tím, že do Internet Exploreru 6 integroval Popup Blocker - k malé radosti inzerentů "třetích stran", jejichž programy se tak stávají zbytečnými.

Svůj browser osvobodíte od vnucujících se pop-upů takto: Pod "Nástroje" zvolte nový bod "Blokování automaticky otevíraných oken". Klepnutím myši zaškrtněte "Zapnout blokování automaticky otevíraných oken", čímž zabráníte automatickému otevírání dalších instancí. To však má tu nevýhodu, že se pak už nezobrazí ani eventuální zajímavá okna. Proto otevřete "Nástroje | Blokování automaticky otevíraných oken| Nastavení blokování automaticky otevíraných oken...", kde můžete definovat výjimky z pravidla. Zadejte doménu, z níž chcete "vyskakovací okna" dovolit, a stiskněte "Přidat".

Volbou "Blokovat všechna automaticky otevíraná okna" znemožníte zobrazení jakýchkoliv oken. Dokonce takových, která musíte extra otevírat klepnutím myši, například reklamních bannerů.

Tip: Pod "Oznamování a úroveň filtrování" zaškrtněte "Při blokování automaticky otevíraného okna přehrát zvuk". Pak při každém zablokovaném okně uslyšíte akustický signál a nepropásnete žádnou eventuálně důležitou webovou informaci. Klepnutím na symbol pop-upu vpravo dole v Internet Exploreru aktivujete nabídku "Blokování automaticky otevíraných oken", kde můžete pop-upy uvolnit, nebo zablokovat.

SPRÁVA PŘÍDAVNÝCH MODULŮ - DOPLŇKŮ

Mnohé programy, ať už chcete, nebo nechcete, se samy připojují k Internet Exploreru. Patří k nim např. Windows Messenger, ICQ, Google Toolbar a Macromedia Flash. Na browser se však může nepozorovaně zavěsit i různý "spyware", jako třeba plug-in "Alexa". Dokonalý přehled vám od nynějška zajistí vylepšená správa "addons". Díky ní můžete přídavné programové moduly ("plug-iny") Internet Exploreru jedním klepnutím rychle a komfortně odstranit nebo připojit. Správce s kompletním přehledem všech "hostujících" programů vyvoláte prostřednictvím voleb "Nástroje | Spravovat doplňky...".

Trochu lepší je strukturovaný přehled, k němuž dojdete v okně Spravovat doplňky přes "Zobrazit | Doplňky aktuálně zavedené v aplikaci Internet Explorer". V něm jsou přídavné moduly roztříděny na "Zapnuto" a "Vypnuto". Chcete-li některý z nich odpojit, vyberte v seznamu příslušnou položku a zvolte položku "Zakázat". Jedná-li se o modul ActiveX, stačí klepnout na "Aktualizovat prvek ActiveX", čímž se browser uvede do aktuálního stavu. V případě všech ostatních modulů musíte Internet Explorer znovu nastartovat.

Tip: Nejprve deaktivujte najednou všechny moduly, které nedokážete jednoznačně přiřadit, a aktivujte je teprve v případě potřeby. Tak zvýšíte bezpečnost a ušetříte systémové zdroje.

ZABEZPEČENÍ INTERNET EXPLORERU

Se svým více než devadesátiprocentním tržním podílem je Internet Explorer bezkonkurenčně nejrozšířenějším webovým prohlížečem a jako takový také nejoblíbenějším terčem pro hackery. Otevřete bezpečnostní nastavení pod "Nástroje | Možnosti Internetu..." a vyberte záložku "Zabezpečení".

- Falešné přípony souborů: Nově přibylo nastavení "Otevírat soubory podle obsahu, ne podle přípony souboru" po stisku Vlastní úroveň v okně Nastavení zabezpečení. To má například zabránit poměrně častým pokusům trojských koní vydávat se třeba za obrazové soubory.

- Cross Site Hacking: Pomocí volby "Webové servery ve více omezené zóně obsahu budou moci přejít do této zóny" chce Microsoft odzbrojit hackery, kteří se pomocí nového okna snaží vniknout do nějaké hůře chráněné bezpečnostní zóny.

- Bezpečnost intranetu: Další krok správným směrem představuje možnost konfigurovat bezpečnostní zónu pro lokální síť. Tak lze mnoho hackerských útoků už předem vyloučit.

Tip: Pod záložkou "Zabezpečení" klepněte na "Úroveň zabezpečení této zóny" a zvolte "Střední". Tam jsou bezpečnostní opatření dostatečně silná.

BEZPEČNÉ ČTENÍ E-MAILŮ

V boji proti e-mailovým červům z internetu Microsoft obohatil Outlook Express o nové ochranné mechanismy, které byly až dosud výsadou jeho velkého bratra Outlooku. Sice dosud stále není k dispozici antispamový filtr, zato však už je možné nechat si e-maily standardně zobrazovat jako čistý text, a ne jako (interpretované) HTML. Díky tomu se skripty, které se dříve automaticky aktivovaly, už nedostanou ke slovu.

Aktivujte volbu "Nástroje | Možnosti..." a v záložce Čtení zaškrtněte "Číst všechny zprávy jako prostý text". Pokud byste si nějaký e-mail chtěli přece jen prohlédnout ve správné podobě HTML, zvolte "Zobrazit | Zpráva ve formátu HTML" nebo stiskněte klávesovou kombinaci Alt+Shift+H.

Dalším bezpečnostním opatřením je možnost nedovolit automatické ukládání obrázků z externích zdrojů. Důvodem je skutečnost, že zasílatelé spamů vytvářejí odkazy na neviditelné, jeden pixel velké "obrazy". Ty se ukládají spolu se zprávou a lze tak zjistit, zda je e-mailový účet ještě aktivní. Pokud zpráva takové přílohy obsahuje, od nynějška se objeví zpráva, že obrazy byly zablokovány. Jsou-li tam přítomny objekty, které byste chtěli vidět, můžete je dodatečně uložit klepnutím na políčko zobrazené v hlavičce e-mailu.

Tip: Pokud chcete tak jako dříve obrazy rovnou ukládat, v "Nástroje | Možnosti..." najdete pod záložkou "Zabezpečení" poněkud "utajenou" možnost deaktivovat "Blokovat obrázky a další externí obsah v e-mailech ve formátu HTML", tedy zrušit zákaz ukládání obrázků.

VYUŽITÍ FIREWALLU WINDOWS

Dřívější ochranu, známou pod názvem "Internet Connection Firewall" (ICF), Microsoft podstatně vylepšil. V rámci bezpečnostní iniciativy je teď firewall standardně aktivován pro všechny síťové karty. Kromě toho je Windows Firewall aktivní už při bootování systému. Až dosud počítač po celou tuto relativně dlouhou dobu "visel" na síti zcela nechráněn. Tak je zabezpečen proti infekcím od Blasteru nebo jiných červů.

Chcete-li změnit nastavení firewallu, klepněte pravým tlačítkem myši na "Místa v síti" a zvolte "Vlastnosti". Potom poklepáním otevřete "Vlastnosti" některého z připojení LAN. Pod záložkou "Upřesnit" klepněte na "Nastavení..." firewallu internetových připojení. Pod záložkou "Obecné" rozhodněte, zda firewall má být "Zapnuto", "Vypnuto", nebo dokonce "Zapnuto, nepovolovat výjimky". V případě poslední volby nedovolí Windows Firewall žádné spojení.

Pod záložkou "Výjimky" najdete všechny aplikace, jimž dovolujete vytvářet připojení do internetu, případně z internetu přijímat data. Jakmile se pokusí otevřít spojení nějaká dosud neznámá aplikace, Windows Firewall se nyní zeptá, zda to chcete dovolit. Tato funkce je známa i z jiných personálních firewallů, jako jsou např. ZoneAlarm nebo Symantec Firewall.

Tip: Kdo využívá pouze firewall a může oželet různé speciality programu ZoneAlarm a podobných, tomu postačí bezplatný Windows Firewall.

SPRÁVA BEZPEČNOSTNÍCH NÁSTROJŮ

V novém "Bezpečnostním centru" sdružuje Microsoft všechny důležité nástroje. Najdete tam Windows Firewall, "automatický update Windows", a dokonce i váš virový skener. Ten ovšem nepochází od Microsoftu, a aby tedy byl rozpoznán, musí "oslovit" určité rozhraní. Pokud se to nepodaří, Windows XP nesprávně oznámí, že žádný "zabiják virů" není nainstalován. V našem testu se tak stalo v případě programu Norton Antivirus. Také cizí firewally zaregistruje Bezpečnostní centrum, jen pokud používají rozhraní. Lze však předpokládat, že v budoucnu budou toto usnadnění práce podporovat všichni výrobci.

Bezpečnostní centrum najdete v symbolické podobě štítu na hlavním panelu vedle hodin. Je-li však váš počítač s Windows XP přihlášen v nějaké doméně, Bezpečnostní centrum neexistuje. Microsoft totiž předpokládá, že v doméně se o bezpečnost počítače stará administrátor, a takové zařízení by proto nemělo smysl.

Valentin Pletzer, autor@chip.cz

DOSTUPNOST SP2 PRO WXP

V době uzávěrky tohoto čísla Chipu Microsoft oznámil, že právě uvolňuje Service Pack 2 pro Windows XP do výroby. Snažili jsme se aktuální plnou verzi SP2 Eng získat na náš CD, bohužel politika

Microsoftu tento způsob šíření SP2 z důvodu bezpečnostních pravidel neumožňuje. SP2 bude k dispozici buď na CD, který Microsoft přislíbil rozesílat uživatelům podle jejich požadavku, anebo prostřednictvím webu. V tento okamžik je ke stažení anglická verze SP2, určená pro instalaci na více počítačů prostřednictvím sítě. Nejsnazší cestou, jak získat SP2 pro jednotlivý počítač, je pro koncového uživatele zapnout Automatický Update. Jeho prostřednictvím se SP2 nainstaluje. Česká verze SP2 je zatím ve fázi přípravy, její uvolnění Microsoft předpokládá v průběhu podzimu tohoto roku. Sledujte Chip.

EXECUTION PROTECTION

HARDWARE CHRÁNÍ XP

Service Pack 2 propůjčuje Windows XP mimo jiné také "ochranu před spuštěním" (Execution Protection). Ta v principu zabraňuje provedení (odstartování) programového kódu. Za tím účelem označí celou paměť příznakem NX ("NX flag", No execute). Pouze v případě, že programový kód zapsaly do paměti samy Windows, je pro příslušnou oblast tento příznak deaktivován. To znamená, že pokud se hacker pokusí prostřednictvím kódu pro přetečení bufferu (Buffer Overflow Code) zapisovat do oblastí, které nejsou takto uvolněny, kód se jednoduše nespustí - útok tak ztratí "půdu pod nohama". Samozřejmě však procesor musí "execution protection" podporovat; výzvu dal AMD s Athlonem 64, Intel oznámil, že se přidá.

Problém: Programy, které nedodržují zásadu oddělení dat od programového kódu, havarují. Tady pomůže jen vypnutí funkce v Ovládacích panelech "Systém" pod "Upřesnit | Výkon | Nastavení".