

# ZÁPLATOVÁNÍ: PODCEŇOVANÉ, LEČ DŮLEŽITÉ

Aktualizace, aktualizace, aktualizace... Stále se bohužel ukazuje, že řada problémů je způsobena tím, že ochranné nástroje jsou zastaralé.

## DNEŠNÍ BEZPEČNOSTNÍ MECHANISMY

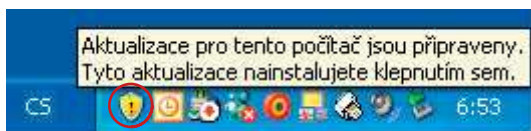
(firewally, antivirové programy, ochranné prvky v internetových prohlížečích apod.) mají velmi slušnou úroveň. Největší nebezpečí tedy nepředstavují tyto programy samy o sobě, ale chyby v nich obsažené.

## DNES JSME NA TOM LÉPE

Není to tak dávno, co softwarové firmy vydávaly své produkty za zcela bezchybné a bezproblémové. Přestože se chyby a problémy evidentně vyskytovaly, vždy se sváděly na „objektivní příčiny“ nebo na cokoliv jiného. Situace se ale změnila, většina výrobců softwaru zcela bez uzardění připouští, že jejich programy mohou obsahovat chyby. Ostatně, není se ani čemu divit – každý počítač na světě je unikátní kombinací softwaru, hardwaru a jejich nastavení, přičemž testování programů probíhá pouze na velmi úzkém vzorku strojů.

Výrobci softwaru si navíc uvědomili, že budou-li k těmto nedostatkům zaujímat pozici „mrtvého brouka“, jednoho krásného dne se jim to nemusí vyplatit. Například poškozený klient je bude žalovat nebo ztratí důvěru významných zákazníků. I z tohoto pohledu se jako přijatelnější jeví možnost existenci chyb připustit, pravidelně je opravovat (hle, služba zákazníkům!) a zodpovědnost tak přenést právě na uživatele.

Samozřejmě že není možné chtít, aby si uživatelé po každé vydané opravě celý program, nebo rovnou operační systém přeinstalovali. A tak vznikly právě patche – záplaty. Jedná se o menší programy nebo soubory, jejichž cílem je po aplikaci na příslušném počítači upravit zdrojové kódy mateřského programu a jeho konfiguraci tak, aby se odstranily známé problémy. Ty mohou být několikrát – kolize příslušného programu s jiným, v některých případech špatná funkce, nechtěná vlastnost, kterou mohou využít hackeři nebo viry, apod.



Na nové záplaty připravené ke stažení ukazuje ikona.

## JAK ZÁPLATY ZÍSKAT

Jak se takové záplatování provádí? V případě nejrozšířenějšího operačního systému je nejjednodušší navštívit stránky [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com) a zde už postupovat podle zobrazených instrukcí. Skript v této stránce totiž samočinně zkontroluje stav záplat na příslušném počítači a ke stažení a k instalaci nabídne záplaty chybějící. Byť některé záplaty mají velikost desítek MB, jejich nasazení je více než žádoucí. Jinak je váš počítač zranitelný, pokud jde o chyby a útoky známé všem hackerům na světě.

## LEGÁLNÍ SOFTWARE JE VÝHODOU

À propos, instalaci některých záplat na počítače s nelegálně nainstalovaným operačním systémem společnost Microsoft blokuje, takže majitelům pirátských Windows je „odměnou“ také zvýšený počet bezpečnostních problémů.

## UŽITEČNÝ BEZPLATNÝ NÁSTROJ

Velice zajímavým a užitečným nástrojem, který je určen pro správu záplat (ale i dalších bezpečnostních parametrů) na nejrozšířenějších operačních systémech, je MBSA (Microsoft Baseline Security Analyzer). Příjemné je, že je k dispozici zdarma. Mezi jeho další klady patří příjemné grafické rozhraní, snadnost obsluhy a konfigurace.

Nové aktualizace získáte na

<http://windowsupdate.microsoft.com>.

Nástroj Microsoft Baseline Security Analyzer

můžete stáhnout z internetové adresy

<http://www.microsoft.com/technet/security/tools/mbsahome.aspx>.

info

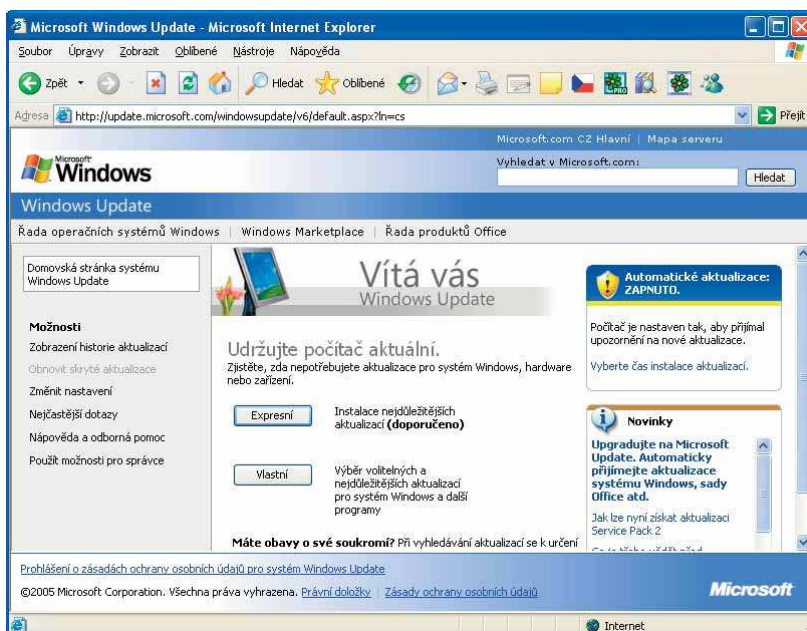
Jedinou výtkou je snad skutečnost, že není k dispozici v češtině, což může některým uživatelům působit určité potíže.

Použití MBSA je velice jednoduché a intuitivní. Jeho nejnovější verze 1.2.1 dokáže kromě (ne)přítomnosti bezpečnostních záplat kontrolovat také další nedostatky, jako např. slabá hesla. To je výhoda oproti službě Windows Update, která sleduje pouze záplaty na úrovni operačního systému.

MBSA funguje na systémech Windows 2000, Windows XP a Windows Server 2003. Krom samozřejmé kontroly těchto platform provádí komplexní kontrolu (i pomocí vzdáleného přístupu) bezpečnostních nastavení a aktualizací Windows NT 4.0 či Internet Exploreru a kancelářského balíku Office. Záběr MBSA v oblasti kontroly záplat je ještě širší a obsahuje kompletní portfolio společnosti Microsoft (Exchange Server, Windows Media Player, MDAC, MSXML, Microsoft Virtual Machine aj.).

Produkt MBSA je určen pro všechny uživatele počítačů, ať již jde o administrátory, či o domácí uživatele. Poslouží všem těm, kteří si chtějí své počítače se systémem Windows udržovat v co nejméně zranitelné konfiguraci. Produkt je možné stáhnout z internetové adresy <http://www.microsoft.com/technet/security/tools/mbsahome.aspx>.

Tomáš Příbyl



Stránky Windows update jsou lokalizované.