

# Nenechejte svá okna zastarat

Radim Peša, ÚVT MU

Opravy bezpečnostních chyb operačních systémů firmy Microsoft se v posledních měsících objevují v množství dříve zcela neobvyklém. Optimisté jsou rádi, že mohou provozovat bezpečnější software. Škarohlídi v tom vidí pouze potvrzení svého přesvědčení, že software firmy Microsoft je nebezpečný pro své okolí. A správcům počítačových sítí nezbyvá, než se s přívalem oprav vyrovnat a zajistit jejich aplikaci na servery a stanice, které udržují. Bez starosti by však neměli být ani koncoví uživatelé. Z jejich pohledu je minimálně vhodné (a námi velmi doporučované) zajímat se o to, zda právě jejich počítač má nainstalovány aktuální „záplaty“ základního software. Neboť neudržovaný software představuje významné bezpečnostní riziko pro počítač a data každého uživatele.

## 1 Opravy pro systémy MS Windows

Opravy pro operační systémy Windows NT, Windows 2000 a Windows XP a serverové aplikace jsou distribuovány primárně v podobě tzv. *Service Packu*. To jsou větší (obvykle několik desítek megabytů) softwarové balíky, které v sobě kumulují všechny dříve vydané opravy příslušné verze operačního systému či dané aplikace. Mimo oprav chyb mohou obsahovat i implementaci nových funkcí software. Nebývají vydávány častěji než dvakrát za rok. Service Packy jsou kumulativní, takže stačí nainstalovat vždy pouze poslední. Pro zajímavost, verze aktuálních Service Packů pro běžně používané produkty jsou následující:

Operační systém Aplikace	Aktuální verze k 1.3. 2002
Windows NT 4.0	Service Pack 6a
Windows 2000	Service Pack 2
SQL Server 7.0	Service Pack 3
SQL Server 2000	Service Pack 2

Při nalezení bezpečnostní chyby, kterou je potřeba opravit ihned, bývá vydán tzv. *hotfix*. V české terminologii používá Microsoft název

*Aktualizace zabezpečení*. Hotfix je malý softwarový balíček, který obsahuje opravu pouze konkrétní bezpečnostní chyby. Hotfixy jsou vydávány podle potřeby a jejich vydání je oznamováno elektronickou poštou. Pro jeho příjem si stačí zaregistrovat na <http://www.microsoft.com/security> příjem služby Microsoft Security Notification Service. Pro příslušné správce na MU přeposílá ÚVT upozornění o vydávaných hotfixech do skupiny [sec-info@munivut.cz](mailto:sec-info@munivut.cz). Při nahromadění většího počtu aktuálních hotfixů byl již několikrát pro usnadnění správy vytvořen balíček, který kumuluje hotfixy vydané od posledního Service packu. Takové sjednocení více hotfixů bývá nazýváno *Security Rollup Package*.

Rovněž pro operační systémy vycházející z Windows 95 existují softwarové opravy. Není jich tolik jako v předchozím případě Windows NT, Windows 2000 a Windows XP, ale vyplatí se o nich vědět a aplikovat je. Opravy samotné včetně dalších informací jsou k nalezení na adrese <http://windowsupdate.microsoft.com>. Uživatelé Windows 98 a Windows ME mohou ke zjištění informací o tom, které opravy mají či nemají na svém počítači instalované, využít službu Windows Update popsanou dále v tomto článku.

## 2 Opravy pro aplikace z MS Office

Softwarové opravy jsou vydávány i pro aplikace z balíku Microsoft Office. Jsou to samostatné opravy konkrétních chyb (obdobu již zmíněných hotfixů), ale také balíky obsahující více oprav a doplňků, které se nashromáždily za delší období. Tyto balíky jsou nazývány *Service Release*, případně také *Service Pack*. Na rozdíl od oprav pro operační systémy nejsou (!) již tyto opravy kumulativní, takže nestačí instalovat pouze poslední verzi oprav. Počátkem března 2002 bylo správné pořadí instalací oprav v jednotlivých verzích MS Office následující:

### MS Office 97

1. Service Release 1 (SR-1)
2. Service Release 2b (SR-2b)
3. případné další opravy

### MS Office 2000

1. Service Release 1a (SR-1a)

2. Service Pack 2 (SP-2)
3. případné další opravy

### MS Office XP

1. Service Pack 1 (SP-1)
2. případné další opravy

Základní informaci o tom, která verze Service Packu či Service Release pro balík MS Office je na počítači nainstalována, může uživatel zjistit v příslušné aplikaci (MS Word, MS Excel apod.) zobrazením nabídek menu *Nápo- věda/O aplikaci . . .*. Uživatelé balíků Office 2000 a Office XP mohou pro jejich aktualizaci využít služby na adrese <http://office.microsoft.com/productupdates>, která jim automaticky zjistí, jaké aktualizace mají nainstalované na svém počítači, a nabídne jim k doinstalování zbývajících. Uživatelé Office 97 najdou vydané aktualizace na adrese <http://office.microsoft.com/downloads>.

## 3 Nástroje pro usnadnění aktualizací

Pro správu bezpečnostních oprav a aktualizací operačních systémů MS Windows existuje několik softwarových nástrojů, které mohou být správcům počítačových sítí (ale i samotným uživatelům) velmi užitečné.

### 3.1 Microsoft Network Hotfix Checker

Pro každého správce stanic a serverů Windows NT, Windows 2000 a Windows XP je nepostradatelným nástrojem Microsoft Network Hotfix Checker (HFNetChk.exe). Použitím tohoto nástroje si správce udržuje přehled o instalovaných i chybějících opravách (Service Pack i Hotfix) udržovaných systémů. Po svém spuštění porovná program HFNetchk.exe momentální stav operačního systému s XML databází existujících oprav vydávanou Microsoftem a upozorňuje na opravy, které je potřeba doinstalovat. Spouští se z příkazové řádky a umožňuje analyzovat lokální i vzdálené počítače. Kromě informací o samotné instalaci opravy v systému sleduje program i správnost verzí a kontrolních součtů aktualizovaných souborů. Vedle oprav samotného operačního systému umožňuje tento nástroj analyzovat opravy také pro:

- Internet Information Server 4.0 a 5.0
- SQL Server 7.0 a 2000 (včetně Microsoft Data Engine)
- Internet Explorer 5.01 a vyšší

Detailní popis nástroje i s možností jeho stažení je k dispozici na adrese <http://support.microsoft.com/default.aspx?scid=kb;EN;q303215>.

### 3.2 Qchain

Nepříjemnou vlastností hotfixů je potřeba restartu počítače, na který byla oprava aplikována. Takže při instalaci deseti oprav se může stát, že bude třeba postupně desetkrát restartovat počítač (což je dost nepříjemná představa). Hotfixy je sice možné spouštět s přepínačem `-z`, který zabrání restartu počítače po instalaci, avšak pokud by bylo takto instalováno více hotfixů najednou, výsledkem může být nekonzistentní stav systému.

Pro takové případy je určen softwarový nástroj Qchain. Při jeho použití může administrátor aplikovat libovolný počet hotfixů. Přepínačem `-z` zamezí vyvolávání restartu a nakonec spustí příkaz `qchain.exe`, který zajistí vzájemnou konzistenci oprav.

Nástroj a jeho podrobnější popis je zájemcům k dispozici na adrese <http://support.microsoft.com/default.aspx?scid=kb;EN;q296861>

### 3.3 Windows Update

Distribuční kanál aktualizací a doplňků operačních systémů zaměřený na individuální a domácí uživatele je dostupný na Internetu na adrese <http://windowsupdate.microsoft.com>. Mimo bezpečnostních oprav jsou zde i aktualizace a rozšíření systémů MS Windows, ovladače nových zařízení. Je zde dostupný software pro všechny 32-bitové systémy MS Windows, tj. Windows 95, Windows 98, Windows Me, Windows NT 4.0, Windows 2000 a Windows XP. Zahrnuty jsou i opravy pro Internet Information Server a www-prohlížeč Internet Explorer. Vzhledem k zaměření na domácí uživatele nejsou touto cestou distribuovány opravy pro serverové produkty.

Při použití prohlížeče podporujícího ActiveX se při přístupu na adresu <http://windowsupdate.microsoft.com> automaticky detekuje verze operačního systému klienta, včetně všech na něm již nainstalovaných oprav, a jsou nabízeny přímo ty aktualizace, které je vhodné na počítač doinstalovat. Tato služba není podporovaná ve Windows 95. Jejich uživatelé si musí opravy dostupné na <http://windowsupdate.microsoft.com> vybrat a nainstalovat sami.

### 3.4 Critical Update Notification

Ve Windows XP je implementována vlastnost automatické aktualizace operačního systému přes Internet. Při její aktivaci operační systém automaticky kontroluje, zda jsou na serveru <http://windowsupdate.microsoft.com> dostupné nové opravy a aktualizace systému. Pokud zjistí přítomnost nové aktualizace, může se, v závislosti na svém nastavení, zachovat dvojnásobným způsobem: buď pouze informuje uživatele o existenci nové aktualizace, nebo ji rovnou stáhne a nainstaluje. Podobnou funkčnost je možné doinstalovat i do systému Windows 2000. Ke stažení je dostupná na <http://windowsupdate.microsoft.com> pod názvem *Upozornění na důležité aktualizace systému Windows* (Critical Update Notification).

## 4 Na závěr

Aplikace bezpečnostních oprav operačního systému je jedním ze základních úkolů správce počítačové sítě a měla by být i běžnou starostí každého koncového uživatele. V minulém roce jsme se mohli přesvědčit, že bohužel zdaleka tomu tak není. Masové šíření internetových červů využívajících bezpečnostních chyb v operačních systémech ukázalo, že velmi často zůstávají na počítačích MU neopraveny chyby i dlouhou řadu měsíců po vydání příslušného hotfixu. Po všech negativních zkušenostech proto znovu připomínáme: *Nenechejte svá „okna“ zastarat!* □