Makroviry v dokumentech MS Office

Radim Peša, ÚVT MU

Makroviry jsou specifickou skupinou virů, která se šíří prostřednictvím dokumentu, nikoliv prostřednictvím programů jako „klasické“ viry. Makroviry využívají toho, že dokumenty určitého formátu mohou obsahovat kód, který je spuštěn při práci s dokumentem a který může být virem infikován.

Jak potvrzují statistiky nejčastěji detekovaných virů (např. `http://www.messagelabs.com/VirusEye`), makroviry dnes již nejsou mezi nejvíce se šířícími druhy počítačových virů. Přesto však rozhodně stojí za připomenutí jak hrozba, kterou představují, tak i opatření, kterými se můžeme před nimi chránit. Obecný problém makrovirů můžeme přitom omezit na makroviry, jejichž hostiteli jsou soubory aplikací z balíku Microsoft Office. Existují sice i případy makrovirů pro jiné aplikace a formáty souborů, ale ty spadají spíše do oblasti kuriozit a nebudeme se jimi proto nyní zabývat. Podívejme se, jak s makry v datových souborech nakládají aplikace posledních tří verzí MS Office.

MS Office 97

Při výchozím nastavení je při otevření souboru s makry v aplikacích Word, Excel a PowerPoint uživatel upozorněn na přítomnost makra a má možnost si vybrat, zda se makra v dokumentu mají spustit či nikoli. Upozorňování na makra se zapíná a vypíná v menu *Nástroje/Možnosti*, kartě *Obecné* a políčku „Antivirová ochrana maker“. Bohužel tato vlastnost nebyla v Office 97 implementována bezchybně a existuje několik možných postupů, které umožňují spustit v dokumentu obsažená makra bez ohledu na nastavení Antivirové ochrany maker. Pokud je například makro obsaženo v šabloně, která je k dokumentu připojena, může dojít k jeho spuštění bez upozornění uživatele. Proto je potřeba k základní instalaci MS Office 97 doinstalovat několik později zveřejněných oprav. Všechny tyto opravy jsou dostupné na adrese `http://office.microsoft.com/downloads`.

Z oprav a doplňků dostupných na výše uvedené adrese je žádoucí vždy nainstalovat dva základní balíky oprav:

- Office 97 Service Release 1 (SR-1)
- Office 97 Service Release 2b (SR-2b)

a dále pak opravy chyb vztahujících se k antivirové ochraně maker:

- Word 97 Security Update: Macro Vulnerability
- Word 97 Update: Mail Merge Security
- Excel 97 Security Update:REGISTER.ID
- Microsoft Excel 97 XLM Macro Security Update
- Microsoft Excel 97 SYLK File Security Update
- PowerPoint 97 Update: HTML Script Vulnerability.

MS Office 2000

V MS Office 2000 je implementována nová vlastnost – digitální podepisování maker. Makra v dokumentu mohou být digitálně podepsaná. Uživatel si potom může ve svém nastavení vybrat, jak se má s příchozími dokumenty obsahujícími makra pracovat. Může si definovat odesílatele, jimž důvěřuje a jejichž makra se mohou spouštět, a zakázat spouštění nepodepsaných maker. Pro zjednodušení tohoto nastavení jsou nově definovány tzv. *Úrovně zabezpečení*, které určují způsob nakládání s dokumenty obsahujícími makra.

Při instalaci je automaticky nastavena „Vysoká úroveň zabezpečení“, která je definována následovně: Nepodepsaná makra nejsou spuštěna, uživatel se o jejich existenci vůbec nedoví. Před spuštěním podepsaných maker je uživatel systémem upozorněn a sám si rozhodne, zda chce makro spustit či nikoli. Případně může také odesílatele přidat do seznamu „Důvěryhodných zdrojů“. V takovém případě je příště makro v dokumentu z tohoto zdroje spouštěno automaticky bez dalšího upozorňování. Nastavení úrovně zabezpečení si uživatel může volit v menu *Nástroje/Makro/Zabezpečení*.

Stejně jako u Office 97 se i zde v implementaci antivirové ochrany maker vyskytují chyby, proto je vhodné doinstalovat později vydané opravy. K tomu je výhodné využít služby dostupné na adrese `http://office.microsoft.`

com/productupdates, která automaticky detekuje na koncovém počítači všechny nainstalované aktualizace a nabídne k doinstalovaní ty chybějící.

Office XP (Office 2002)

V Office XP jsou makra v souborech zpracovávána stejně, jak bylo popsáno u MS Office 2000. I když se jedná o relativně nový produkt, implementace antivirové ochrany maker obsahuje chybu popsanou u předchozích verzí a je proto třeba doinstalovat opravu. Ta je zahrnuta v zatím jediném balíku oprav pro Office XP pojmenovaném Service Pack 1. U Office XP je stejně jako Office 2000 podporována služba automatické detekce chybějících oprav dostupná na adrese http://office.microsoft.com/productupdates.

Závěr

Jak je vidět, všechny uvedené verze systému MS Office mají implementován nějaký mechanismus zabraňující samovolnému spuštění makra při otevírání dokumentu. Je vhodné je využívat, mít zakázáno spouštění maker a pouze explicitně jejich spouštění povolovat při otevírání těch dokumentů, u kterých víme, že použití maker je v nich nezbytné. Takové dokumenty by ovšem měly být vždy předem prověřeny antivirovým programem. Bohužel u žádné verze MS Office není mechanismus umožňující výběrové spouštění maker implementován bez chyb. Vždy je proto třeba doinstalovat opravu bezpečnostních děr, které umožňují použitý mechanismus ochrany obejít.

Takže naše závěrečné doporučení zní:

1. Používejte na svém počítači antivirový program a udržujte ho aktuální.
2. Nainstalujte si vydané opravy chyb (a čas od času ověřte, nejsou-li k dispozici nové opravy).
3. Ve všech programech z balíku MS Office mějte trvale zapnutou antivirovou ochranu maker. □