

To nejcennější, co ve svém počítači máte, jsou bezesporu vaše data. A ta je potřeba trvale chránit. Jejich případná ztráta totiž může mít nedozírné následky. Jedním ze způsobů jejich možného poškození nebo ztrát je napadení počítače virem. Proto by měla být samozřejmostí trvalá antivirová ochrana (spolu s pravidelným zálohováním).

Zkáza pro viry

Není to dlouho, co se společnost **AEC** stala na českém trhu distributorem programu **AntiViral Toolkit Pro (AVP)**. Ruský antivirový systém AVP společnosti **Kaspersky Lab** by tak měl být v nejbližší době dostupný i v lokalizované (české) verzi. Do ruky se mi však dostala ještě anglická verze, která je určena pro operační systém Windows 9x/NT (existují však i varianty pro DOS, Windows 3.1x, Novell NetWare a pro Linux).

AVP pro Windows 9x/NT obsahuje klasický skener – *AVP Scanner* – který může uživatel spouštět ručně na vybrané oblasti, anebo jeho spuštění automaticky načasovat pomocí programu *AVP Control Center*. Skener dokáže detekovat snad všechny typy virů, včetně těch, které se šíří prostřednictvím VBScriptů či CorelScriptů (samozřejmostí je i detekce makrovirů). V případě souborových (programových) virů lze využít i heuristickou analýzu, která dokáže detekovat kolem 80 % neznámých virů s minimálním počtem falešných poplachů. Celkově jsou detekční schopnosti antiviru AVP na špičkové úrovni, což dokazují i časté srovnávací testy antivirových programů.

Další silnou stránkou je prohlížení komprimovaných archivů a interně komprimovaných EXE souborů. V testované verzi bylo podporováno přes 15 formátů (!) komprimovaných archivů, mezi kterými samozřejmě nechybí RAR, ZIP, ARJ apod. Další, zcela ojedinělou funkcí je schopnost “zmrazit” virus přímo v operační paměti. Takto “zmrazený” virus se již nedokáže šířit, a není proto nutné zavádět operační systém ze systémové diskety. Zmiňovanou funkci lze s úspěchem využít například při odstraňování viru W95/CIH (Černobyl). Stejně detekční schopnosti nabízí i paměťově rezidentní skener – *AVP Monitor* – který automaticky sleduje spouštěné i otevírané soubory. Příjemným doplňkem je i funkce “Smart”. Pokud je zapnuta, AVP Monitor prohlíží soubory i podle jejich hlavičky. Testem pak projde například i EXE soubor s nestandardní hlavičkou. I u AVP Monitoru lze aplikovat heuristickou analýzu a prohlížení archivů či interně komprimovaných EXE souborů. Informace o nalezeném viru jsou podávány do grafického okna (většina antivirů používá spíše výstup do textového režimu). Infikovaný soubor lze většinou úspěšně “vyléčit” (další opravdu silná zbraň tohoto antiviru), nebo ho smazat.

Jako většina jiných antivirů i AVP nabízí aktualizaci prostřednictvím sítě internet. Antivirus AVP je aktualizován zpravidla každý týden, a to ve formě doplňků. Není tedy nutné pokaždé stahovat celou, stále narůstající databázi virů, ale pouze několik kB dlouhý soubor (doplňek), který rozšíří detekci o viry, jež spatřily světlo světa od posledního doplňku.

A co z toho všeho vyplývá? AntiViral Toolkit Pro je velmi kvalitní antivirový systém, který si jistě najde velké množství spokojených uživatelů.

Aktualita

Na internetové adrese www.aec.cz/Encyclopedia/Index.htm můžete najít AVP Virus Encyclopedia – pohled do jedné z největších encyklopedií o virech a o všem, co s touto problematikou souvisí. Tato trvale aktualizovaná databáze pochází také z dílny “Eugena” Kasperského a obsahuje informace o více než 14 tisících známých i méně známých virů. Nechybí ani trocha teorie a rejstříky pro snazší orientaci.