AVG 6.0

Kto by nepoznal brnenskú firmu Grisoft software, ktorej produkt AVG sa stal v Česku a na Slovensku symbolom antivírusových programov. V súčasnosti má AVG za sebou už takmer 9 rokov vývoja, v priebehu ktorých prechádzal viac či menej výraznými zmenami a pribúdali nové možnosti a technológie. Zásadné zmeny obsahuje aj dlho očakávaná nová verzia označená číslom 6.

Preteky pokračujú

Počiatky počítačových vírusov sa objavili už v šesťdesiatych rokoch, našťastie však len vo fantázii spisovateľov sci-fi literatúry. Až začiatkom osemdesiatych rokov im dal rozvoj techniky reálnu šancu na existenciu, zatiaľ len v laboratórnych podmienkach. Písal sa však rok 1986 a svetlo sveta (alebo bajty programov?) uzrel Brain – prvý skutočný počítačový vírus pre osobné počítače IBM PC. “Zásluhu” na tom mali bratia Basid a Amjad Farooq Alviovci, ktorí prevádzkovali v pakistanskom Lahore malý obchod so softwarom.

Nemajte im to však za zlé. Ak nie oni, určite by sa našiel niekto iný, kto by odštartoval šialené preteky vírusov a antivírusov, na ktorých sa všetci zúčastňujeme dodnes. Od tej doby sa však veľmi veľa zmenilo. Autori vírusov aj antivírusov postupne zvládli špičkové techniky a počítačové vírusy sa rozšírili v takom rozsahu, o akom sa nezdalo ani spisovateľom v najbujnejšej fantázii. Objavili sa vírusy šíriace sa v dokumentoch, a v poslednej dobe aj prostredníctvom e-mailu.

A čo budúcnosť? Isté je len to, že doterajší vývoj vo vírusovom svete sa rozhodne nenachádza vo svojej konečnej fáze. Veď napríklad vďaka tomu, že Microsoft licencoval VisualBasic for Application niekoľkým firmám, sa môžeme veľmi skoro dočkať vírusov nielen v dokumentoch MS Office, ale aj CorelDRAW a ďalších. Našťastie však neprestane ani vývoj v oblasti antivírusových programov (čoho príkladom je aj nové AVG), ktoré doteraz dokázali bez väčších problémov zvládnuť všetky vírusové triky.

Dodávka a inštalácia

V dodávke ***AVG 6.0*** nájdete okrem inštalačného média CD-ROM aj používateľskú príručku, registračnú kartu a objednávku aktualizačnej služby. Používateľská príručka je netradičná – dvojstranná. Z jednej strany je popis inštalácie a prvých krokov s programom, z druhej zaujímavé informácie o počítačových vírusoch (ktoré doporučujem preštudovať). Na inštalačnom CD sa nachádza niekoľko jazykových mutácií AVG. Sú to česká, slovenská (ako vyzerá, vidíte na obrázkoch), anglická a nemecká verzia. Okrem verzie pre Windows 95/98/NT tu samozrejme nájdete aj verziu pre DOS.

Inštalácia verzie pre Windows je jednoduchá a zvládne ju aj úplný začiatočník. V jej priebehu môžete konfigurovať kontroly a zvoliť automatickú aktualizáciu z internetu. Po následnom reštarte

systému pokračujete v konfigurácii možnou okamžitou aktualizáciou, vytvorením záchrannej diskety, prípadne prvým skenovaním. Pokiaľ ste nemenili pri inštalácii žiadne nastavenia, nainštaluje sa okrem samotného programu aj *AVG BOOT-UP Scanner* (kontroluje systémové oblasti a niekoľko základných a systémových súborov pri štarte počítača) a rezidentná ochrana v prostredí Windows 9x/NT.

Pod kapotou

Na prvý pohľad vyzerá AVG 6.0 ako iné antivírusové programy. Hlavný skenovací program pre Windows alebo DOS, VXD driver alebo rezident, e-mail skener, ... Pokiaľ sa však detailne pozriete “pod kapotu”, uvidíte zásadný rozdiel v programovej štruktúre a úplne prepracované testovacie jadro. Doteraz bol každý program z balíka AVG samostatným programom, ktorý mal samostatné testovacie rozhranie. To malo svoju nevýhodu v tom, že napríklad rezidentný program mal iný záber ako skener alebo heuristika. AVG 6.0 má spoločné testovacie jadro vo forme drivera a jednotlivé programy AVG využívajú jeho služby. Výsledok takejto štruktúry AVG je, že každá časť antivírusového systému má rovnakú a plnú testovaciu schopnosť.

Rozhranie

Používateľské rozhranie novej verzie systému AVG je prepracované a prispôsobené rôznym používateľom. Základné rozhranie je určené pre menej skúsených používateľov a tzv. pokročilé rozhranie pre profesionálov.

Základné rozhranie ponúka jednoduché, prehľadné prostredie a zjednodušené ovládanie. K dispozícii máte jednoduchý výber prednastavených testov a jedného používateľsky definovaného testu, prehľad o aktuálnom stave jednotlivých častí AVG, môžete vykonať aktualizáciu cez internet, prípadne naplánovať spustenie testu alebo aktualizácie v určenú dobu.

Pokročilé rozhranie je určené nielen pre pokročilejších používateľov, ktorí majú vedomosti o antivírusovej ochrane, ale aj pre tých, ktorí chcú lepšie prispôsobiť AVG svojím potrebám. Prostredie tvorí okno s ponukou vo forme stromu funkcií, ktoré veľmi dobre poznajú používatelia predchádzajúcej verzie AVG. Jeho prostredníctvom máte prístup k všetkým funkciám AVG.

Honba na vírusy

AVG používa pri detekcii vírusov tri techniky: hľadanie známych vírusov, heuristickú analýzu a sledovanie zmien.

Hľadanie známych vírusov vyhľadáva v súboroch charakteristické znakové sekvencie známych vírusov. Táto metóda je však dnes už málo účinná – používaná bola hlavne v počiatkoch antivírusových programov.

Oveľa účinnejšia je **heuristická analýza**, ktorá dokáže rozpoznať aj nové neznáme vírusy. Jadrom heuristickej analýzy v AVG je emulátor inštrukcií procesoru Intel. Ide vlastne o “virtuálny počítač”, v ktorom si môžete “spustiť” program alebo rôzne systémové akcie, napríklad zavádzanie operačného systému z boot sektoru alebo z MBR pevného disku. Vďaka tomuto emulátoru kódu je úplne jedno, ako zložito zašifrovaný alebo nečitateľne napísaný je testovaný program. V priebehu emulácie prebieha aj

zber informácií o význame emulovaného kódu a AVG sa snaží ich vyhodnotením odhadnúť, či ide o činnosť typickú pre neškodný program, alebo naopak pre počítačový vírus.

Samozrejme ani heuristika nie je všeliek a má určité nevýhody a obmedzenia, ako možné falošné poplachy, neschopnosť identifikácie vírusov napísaných vo vyšších programovacích jazykoch a ďalšie. Firma Grisoft software však neustále pracuje na zdokonalení tejto metódy, čoho dôkazom je napríklad príprava heuristickej analýzy pre makrovírusy.

Pre sledovanie zmien je určený **test integrity**, ktorý dopĺňa vyhľadávanie známych vírusov a heuristickú analýzu. Tento test si ukladá dôležité informácie o súboroch a systémových oblastiach, ktoré sú využívané nielen pri detekcii vírusov, ale aj pri "liečení" súborov.

Samozrejmá je možnosť kontroly súborov v archívoch typu ARJ, ZIP a RAR, v samorozbaľovacích archívoch a v interne komprimovaných spustiteľných súboroch. Novou schopnosťou testovať archívy obsiahnuté vnútri ďalších archívov odstraňuje AVG handicap predchádzajúcej verzie.

AVG obsahuje niekoľko typov štandardných testov, takmer rovnakých ako v predchádzajúcej verzii. Sú to ***Rýchly test*** (systémové súbory, oblasti a súbory spúšťané pri zavádzaní systému), ***Hlavný test*** (základný test AVG), ***Kompletný test*** (obsahuje spoločné nastavenia pre obidve používateľské rozhrania) a ***Test výmenných zariadení*** (kontrola diskiet, CD-ROM a ďalších vymeniteľných médií).

Nechýba ani ***Manažér testov***, ktorý umožní úpravu parametrov existujúcich testov a tiež vytvorenie vlastných testov s rôznymi používateľskými nastaveniami. K dispozícii je tiež ***Plánovač testov***, prostredníctvom ktorého môžete naplánovať automatické spúšťanie vybraných testov v určený čas. Nastaviť tu môžete množstvo parametrov ako čas spustenia, periodicitu, prioritu a podobne.

Tak ako dnes už každý antivírusový systém, obsahuje aj AVG ***rezidentnú antivírusovú kontrolu***. Táto kontrola môže sledovať kopírované súbory, diskety, systémové oblasti, makrovírusy a rôzne iné štandardné a neštandardné aktivity v systéme, a tak odhaliť možné infikovanie vírusom.

Dôležitou súčasťou AVG je ***rozšírenie pre e-mail***, ktoré preveruje pripojené súbory pri príchode k vášmu poštovému klientovi. Preverované sú však aj odchádzajúce správy. Nastaviť tu môžete aj certifikáciu – potom bude AVG v prípade nezistenia vírusu automaticky pripájať k prichádzajúcej a odchádzajúcej správe vami zadaný textový reťazec (napríklad "Prichádzajúca správa neobsahuje vírusy"). Podporované sú programy MS Exchange klient, MS Outlook a Qualcomm Eudora, ďalšie budú pribúdať v aktualizáciách.

Pri **detekcii vírusu** v súbore ponúka AVG viacero možností – pokračovať ďalej, liečiť súbor, prípadne ho zrušiť (chýba mi tu však možnosť premenovania súboru). Liečenie je kombináciou niekoľkých funkcií a vo väčšine prípadoch je úspešné. Pokiaľ však AVG nájde vírus, ktorý nevie liečiť, presunie ho do "vírusového trezoru". Ide o špeciálny adresár určený pre ukladanie napadnutých súborov, ktoré sú v tomto adresári premenované a zakódované. V prípade potreby ich môžete zrušiť, obnoviť alebo liečiť (napríklad po aktualizácii, s ktorou AVG dokáže obsiahnutý vírus liečiť). Určite by sa však hodila aj možnosť automaticky odoslať napadnutý súbor napríklad priamo firme Grisoft na analýzu.

Vírusom napadnutú *systémovú oblasť* je samozrejme možné len liečiť. Pritom sa využívajú údaje z databázy rýchleho testu. Pokiaľ toto nie je úspešné, použije sa obnovenie systémovej oblasti nahradením napadnutého kódu. Pri použití diskových nástrojov, ako napr. EZ-DRIVE, však táto možnosť nebude úspešná.

Pre núdzové situácie je k dispozícii **vytvorenie záchrannej diskety**, ktorá už neobsahuje len zálohy systémových oblastí, ale tiež možnosť štartu systému z tejto diskety a spustenie AVG v režime SOS s možnosťou obnovy systémových oblastí a liečenia.

Pri antivírusových programoch je obzvlášť potrebná ich pravidelná **aktualizácia**. AVG rieši automatickú aktualizáciu prostredníctvom internetu. Aktualizovať môžete tiež "ručne", a to z internetu, adresára alebo CD. Kto nemá prístup k internetu, môže si objednať aktualizačnú službu.

Aj pre DOS

Ani v AVG 6.0 nechýba verzia určená pre DOS. Prostredie sa oproti predchádzajúcej verzii takmer nezmenilo, testovacie možnosti sú vďaka využívaniu rovnakého testovacieho jadra totožné s verziou pre Windows.

Aj v prostredí DOS je dostupná **rezidentná ochrana**, a to vo forme DOS drivera AVGSYS. Nastaviť jeho vlastnosti je možné prostredníctvom parametrov na príkazovom riadku.

K dispozícii je aj maximálne zostručnená verzia AVG pre DOS – verzia ***AVG/SOS***, ktorá slúži v havarijných prípadoch na spustenie zo záchrannej diskety. Obsahuje len funkcie na testovanie a liečenie, na obnovu z vírusového trezoru a na obnovu systémových oblastí, ako aj informácie o inštalácii AVG.

Záver

Nová verzia AVG splnila takmer všetky očakávania. Možnosti testov a funkcií, veľmi potrebná kontrola elektronickej pošty, automatická aktualizácia, príjemné prispôsobiteľné prostredie a jednoduché ovládanie z nej tvoria vynikajúci antivírusový systém, ktorý sa nepochybne radí k svetovej špičke. Nezanedbateľná je tiež technická podpora používateľov a ďalšia nová verzia AVG zdarma pre registrovaných používateľov.

O kvalitách systému určite svedčí aj certifikovanie renomovanou spoločnosťou ICSA *(www.icsa.net)*.

Štefan Stieranka