AVG Anti-Virus plus Firewall

Firewall a antivirus v jednom. Vede tudy cesta k bezpečné budoucnosti?

VOJTĚCH BEDNÁŘ

Bezpečnostní software je součástí nezbytného minima výbavy PC již řadu let. Množství hrozeb prudce stoupá, ruku v ruce s rozmachem internetu a jeho stále větší penetrací mezi „nepoučené“ uživatele. Myšlenka vzájemné integrace antiviru a firewallu se tedy nabízí sama.

Kombinované bezpečnostní aplikace spojující více funkcí vyrábí řada světových společností. Nyní se k nim řadí i česká firma Grisoft – výrobce antivirového programu AVG.

Nedávno nám Grisoft nabídl k testování betaverzi kombinovaného produktu, antivirového systému a osobního firewallu v jednom, s názvem „AVG Anti-Virus plus Firewall Edice“. Jeho účelem je dosáhnout zjednodušení počítačové bezpečnosti. Jak starý antivirus s novým firewallem vypadá a co všechno umí? Na to se nyní můžete podívat spolu s námi.

2 v 1? Proč ne, proč ano?

Účel antivirového systému je jasný: vyhledávat a eliminovat rizika způsobená škodlivým softwarem z internetu a z datových nosičů. Přestože různých virů a červů existují desetitisíce a metod, jak se mohou dostat do počítače, také mnoho, v poslední době mezi nimi hraje prim šíření pomocí elektronické pošty.

Stejně jako existují tisíce virových hrozeb, jsou i desítky antivirových aplikací. V praxi se ale na určitém území, respektive mezi určitým typem uživatelů/správců IT setkáváme jen s několika vybranými produkty. V zemích jako je ta naše jsou upřednostňovány systémy, které „hovoří“ domácím jazykem, zvláště pak ty vyvíjené tuzemskými silami. Výjimkou je v našem případě ne tak úplně tuzemský, leč velmi kvalitní NOD32.

Vzhledem ke způsobu šíření většiny nových infekcí (ať tak či onak, většinou po síti) dochází k prolínání funkcí antivirového systému a firewallu. Účelem firewallu je omezovat provoz síťových služeb, aby nemohly být využity pro útok na aktivní objekt v síti (v našem případě počítač) a pokud k takovému útoku dojde, pak mu zabránit. Z těchto důvodů je třeba monitorovat síťový provoz. K témuž je ale odsouzen i antivirový program. Přibližně zde se nachází počátek myšlenky spojení obojího dohromady.

Kombinace antivirového systému s osobním firewallem má i další přednosti. Jeden systém místo dvou se lépe spravuje, lze ho centrálně aktualizovat a vůbec udržet pod kontrolou. Pro uživatele i pro správce představuje homogenní bezpečnostní prvek. Dvě komponenty, které jsou přímo či nepřímo nuceny spolupracovat, to budou dělat lépe, pokud se „znají“ již z výroby. Výsledkem by měla být vyšší bezpečnost v jednodušším balení.

Kombinace více bezpečnostních funkcí do jednoho balíčku má ale i své nedostatky. Chyba v jednom produktu se může negativně promítnout do činnosti druhého. Úspěšný útok či hack jedné části znamená vyřazení obou. Celkově se ale dá říci, že integrace bezpečnostních prvků je dobrý nápad a Grisoft se vydal ověřeným směrem, který představuje jednu z vizí budoucnosti zabezpečení ve stylu „všechno v jednom“.

Co je to?

AVG Anti-Virus plus Firewall Edice je kombinace antiviru AVG7 a osobního firewallu v jednom uživatelském rozhraní a jednom balíku.
URL: *www.avg.cz, www.grisoft.cz*
Cena: do uzávěrky neznámá, betaverze.

Klady a zápory

- ☺ „2 v 1“
- ☺ jednotné ovládání, odpadá nutnost používat dva produkty
- ☺ podrobná konfigurace jádra firewallu, mnoho voleb
- ☺ systém šablon a skenování
- ☹ stabilita betaverze

Instalace a start

Balík antiviru a firewallu zabírá v celkové instalaci přibližně 16 MB. Po spuštění je zahájena standardní instalace, během níž je možné vybrat si z uživatelského a expertního režimu, který zcela logicky nabízí větší paletu voleb. Po dokončení instalace je nutné provést automatickou konfiguraci přibaleného firewallu, která spočívá nejprve ve skenování obsahu počítače. Po jeho dokončení je uživateli zobrazen seznam protokolů, které jsou nainstalovány, s tím, že je možné si vybrat, pro které z nich je potřeba vytvořit patřičné pravidlo. Ostatním jsou pak přiřazena oprávnění podle nastavení politiky firewallu.

Jak AVG antivirus (již tradičně), tak i firewall jsou rozpoznávány centrem zabezpečení operačního systému Windows. To je důležité, protože to znamená dokonalou kompatibilitu nového produktu s aktualizací servisních balíčků Windows.

Aplikace, ovládání, antivirus

AVG Anti-virus plus Firewall Edice vychází ze známějšího antiviru a tomu se podřizuje i jeho charakter. Pokud jste někdy pracovali s AVG, budete se v prostředí komba pohybovat jako ryba ve vodě. Základem systému je manažer AVG Control Center. V něm jsou zobrazeny jednotlivé komponenty, včetně jejich stavu. K výběru jsou zde základní administrační kroky, aktualizace a především možnost otevřít podrobná nastavení jednotlivých modulů a jejich komponent či provést ověření systému antivirem.

Pokud jde o antivirovou část systému, k dispozici jsou standardní komponenty, tedy provádění testů, plánování, práce s virovým trezorem a nezbytná kontrola pošty. Hlavní část nabízí dvě uživatelská rozhraní. Jedno zjednodušené, s nabídkou funkcí testování počítače formou velkých a vůči chybnému zásahu dobře odolných tlačítek, a jedno pokročilé s lepšími možnostmi nastavení. Záleží na uživateli, jaké si vybere – efekt vyhledávání virů by měl být stejný.

Celkově vzato v antivirové části systému není nic nového, co by uživatele znalého AVG mohlo překvapit.

Firewall poprvé

S firewallovou částí AVG Anti-virus plus Firewall Edice jsme se setkali zatím jen při instalaci v podobě konfiguračního průvodce. Po zavedení se firewall chová jako jeden z modulů antivirového systému. Cesta k němu tedy vede přes kontrolní centrum AVG, kde jsou tři základní akce. První z nich je zastavení nebo obnovení provozu firewallu, druhou zobrazení jeho vlastností a třetí pak vlastní konfigurace firewallu.

Ve vlastnostech najdeme okno s rozšířenou možností zastavení či vypnutí firewallu, ale také indikátor aktuálního stavu, čísla verze a data jejího sestavení. K dispozici je otevření protokolu firewallu, do něhož jsou zaznamenávány důležité události, nebo otevření konfigurace – stejně jako ze samotného kontrolního centra.

S nastavením firewallu lze pracovat v zásadě dvojím způsobem. Po pouhém otevření konfiguračního dialogu je zobrazen seznam známých aplikací s možností jejich konfigurace. U každé si můžeme vybrat chování firewallu, tedy zda bude aplikaci povolen či zamítnut přístup k síti. K dispozici je možnost ruční editace seznamu ve smyslu přidávání či odstraňování aplikací. Zatímco některé firewally vyžadují na počátku „učící“ se režim, v němž je seznam aplikací naplněn uživatelskými odpověďmi na dotazy systému, v tomto případě jsou do seznamu převedeny aplikace a nastavení, jež byly nalezeny během úvodního skenování počítače.

Tato skutečnost konfiguraci značně zjednodušuje, avšak obligátní otázka na povolení síťového provozu je stále přítomna a firewall ji v případě méně známé služby neváhá položit. Pokud se uživateli zobrazí, prakticky ničím se neliší od konkurence – okno s názvem aplikace, možnost povolení nebo odmítnutí přístupu k síti, možnost vytvoření pravidla, a to je vše.

Tolik k základnímu nastavení, ale firewall v AVG toho umí mnohem více. Po aktivaci „detailů“ můžeme u jednotlivých aplikací nastavovat pravidla pro každou síťovou službu zvlášť. Pro jednotlivé aplikace, respektive služby je možné definovat, které z instalovaných síťových adaptérů může daná služba využívat. Jednotlivé služby je možné zvlášť protokolovat, což ocení zejména správci systémů, protože tato funkce nahrazuje činnost některých administračních nástrojů. Služby, které systém nezná nebo v něm nejsou přítomny, lze podrobně konfigurovat zadáním základního protokolu, směru komunikace a používaného portu. K dispozici je možnost klonování známých služeb – opět užitečný nástroj.

Jinými slovy: konfigurace a nastavení AVG firewallu je buď velmi jednoduché, nebo velmi podrobné. První z nich je ideální pro uživatele, druhá nadchne administrátora, protože je v mnohém lepší než například u populárního Zone Alarmu.

Ve firewallu je možné vytvářet „sítě“, tedy oblasti IP adres se společnou politikou. I tento detail je vyřešen jednoduše a velmi efektivně a Grisoft za něj chválíme.

Firewall podruhé

Firewall jsme tedy úspěšně konfigurovali a nezbývá, než jej začít používat. Zde se opět projevilo několik nedostatků, souvisejících pravděpodobně s betaverzí. Mezi ně patří opakované dotazování na známé aplikace a také bohužel občasné pády, spojené s odpojováním počítače od sítě. Blokování nicméně funguje precizně, což musíme ocenit zejména u selektivní varianty (tedy té, kdy jsou pro různé směry a protokoly v rámci různých aplikací nastavena odlišná pravidla). Nedostatkem je také nemožnost zablokovat konkrétní adresu (site) jinak, než pomocí editoru sítí přímo z firewallu. Tím ale výčet nedostatků víceméně končí, protože další výraznější chyby se nám v tomto produktu, s přihlédnutím ke skutečnosti, že se jedná o betaverzi, najít nepodařilo.

Celkové hodnocení

Pokud používáte AVG antivirus a osobní firewall, pak nový kombinovaný produkt vypadá lákavě. Integrovaný firewall nevyniká bombastickým uživatelským rozhraním nebo skvělými efekty. Je spíše jednoduchý, ale zase dělá přesně to, co má. Současně nabízí jak jednoduchou, tak i velmi pokročilou možnost konfigurace a precizní záznam událostí. 5 0403/BAM ❑

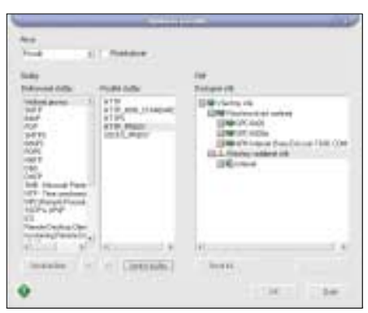
▲ **Klasická otázka na program, stejná jako u konkurence.**

▲ **Aktualizace je stejná jako u ostatních částí AVG.**

▲ **Skenování po instalaci – nastavení aplikací.**

▲ **Nastavení aplikací v hlavním okně firewallu.**

▲ **Před skenováním.**



▲ **Pokročilé nastavení nabízí bohaté možnosti.**

▲ **Kontrolní centrum bezpečnosti AVG.**

▲ **Nastavení protokolu po instalaci.**