KROK PO KROKU PORADNIK

Tomasz Szetyński

Zabezpiecz komputery sieci firmowej

Fot. Kwerry

Nie tylko antywirus, lecz kompleksowe rozwiązania

Bezpieczeństwo systemów informatycznych jest niezwykle ważnym zagadnieniem w świecie, w którym codziennie wymieniamy miliony gigabajtów danych za pośrednictwem sieci komputerowych. Nie tak dawno jeszcze bezpieczeństwo komputera gwarantował w większości przypadków program antywirusowy. Dzisiaj jednak mówiąc o kwestiach zabezpieczeń do popularnego „antyvira" dodać jeszcze musimy programy typu *firewall*, *antyspyware* oraz *antyspam*. Co więcej, owo zainstalowanie wyżej wymienionych programów może okazać się niewystarczające, jeżeli nie zadbamy o to, by na naszym systemie operacyjnym instalować okresowo ważne z perspektywy bezpieczeństwa aktualizacje, nazywane często przez producentów programów „krytycznymi". Proces ten, nazywany potocznie „łataniem dziur" lub instalacją „łat" dotyczy także każdego rodzaju oprogramowania zainstalowanego w systemie operacyjnym.

Co wyróżnia pakiety *Internet Security*

W składa pakietów określanych mianem *Internet Security* wchodzą zazwyczaj: program antywirusowy, *firewall*, program antyspamowy, a także w zależności od producenta także program zabezpieczający nas przez złośliwymi programami i szpiegami typu *spyware*, ochrona kont systemu Windows, ochrona osobistych (prywatnych) danych – numerów kart kredytowych, haseł, czy innych ważnych danych, a także tzw. „ochronę rodzicielską", której zadaniem jest filtrowanie treści niedozwolonych dla dzieci umieszczanych na stronach WWW. Dodatkowy moduł takiego pakietu może stanowić program *antiphishing*, którego zadaniem jest zabezpieczenie użytkownika przed oszustwami internetowymi. Program taki filtruje wiadomości e-mail zawierające potencjalne zagrożenia w postaci linków do fałszywych stron internetowych, gdzie kradzione są np. informacje bankowe.

Przed zakupem takiego pakietu warto wiedzieć, jakie cechy powinien posiadać każdy program wchodzący w jego skład. Zacznijmy od cech samego programu antywirusowego, którego jedną z najważniejszych funkcji jest ochrona systemu w czasie rzeczywistym (*auto-protect*), a polega na tym, że „silnik" antywirusa skanuje w tle poszczególne pliki zapisane na dysku twardym na obecność wirusów. Antywirus skanuje nie tylko pliki, ale również wszystkie programy, które właśnie otwieramy, a więc w ten sposób jesteśmy chronieni przez zarażeniem wirusem, kiedy przypadkowo otworzymy plik nieznajomego pochodzenia. Kolejną podstawową, a zarazem bardzo ważną funkcją jest skanowanie poczty w programach pocztowych – zarówno tej przychodzącej, jak i wychodzącej z naszego komputera. Kiedy ściągamy e-mail, który zawiera załączniki, czy linki do stron WWW nasz program antywirusowy automatycznie sprawdzi go, czy nie zawiera niebezpiecznego oprogramowania mogącego uszkodzić nasz system i dane. Jak wiadomo nowe wirusy są wymyślane przez ich twórców w zawrotnym tempie, dlatego każdy program antywirusowy powinien mieć również opcje automatycznej

aktualizacji baz wisusów, gdyż wtedy jesteśmy pewni, że jesteśmy chronieni przez wszystkimi typami wirusów, w tym również tymi najnowszymi. Nowoczesne pakiety dla kompleksowej ochrony komputera posiadają również moduł *antispyware*, który chroni przed programami szpiegującymi.

Jeszcze jedną cecha programu antywirusowego, na którą musimy zwrócić szczególną uwagę to „kwarantanna". Jest to miejsce, do którego trafiają zarażone pliki, a z których program antywirusowy w danym momencie nie jest w stanie usunąć wirusa. Jest to o tyle istotne, że pliki zainfekowane bardzo często zawierają ważne dane, i nie możemy ich po prostu usunąć, aby pozbyć się wirusa.

W dalszej kolejności przyjrzyjmy się poszczególnym cechom programu *firewall*, który powinien zawierać funkcje: alerty o infekcji, osobistych ustawień zapory indywidualnie dla każdego programu, który łączy się z siecią Internet, zabezpieczenie przed włamaniami, a także kontrolę prywatności, która będzie chronić nasze szczególnie cenne dane jak: hasła, czy np. numery kart kredytowych. Oczywiście nie jest możliwa dobra ochrona komputera, bez współpracy programu antywirusowego z programem *firewall*, dlatego najlepiej jest, gdy oba te programy pochodzą od jednego producenta, gdyż wtedy mamy zapewnioną idealną współpracę.

Niechciane maile precz!

Aby uchronić się przez napływem niechcianej korespondencji, która krąży w Internecie w ogromnych ilościach, warto zwrócić uwagę, aby nasz pakiet ochronny posiadał także moduł antyspam, który w miarę możliwości skutecznie zlikwiduje problemem nie chcianych wiadomości e-mail, zaś same adresy e-mail pozwala klasyfikować według „czarnej i białej listy".

Przegląd najlepszych programów zabezpieczających

Programy przedstawione w tabeli, to rozwiązania, które najskuteczniej chronią zasoby komputera i sam system przez wirusami i innymi zagrożeniami. Są to rozwiązania kompleksowe typu *Internet Security*, które we wszystkich testach programów zabezpieczających zajmują miejsca w pierwszej dziesiątce. Jednym z najbardziej popularnych w naszym kraju jest program **Norton Internet Security 2006** firmy Symantec. Jest to program w polskiej wersji językowej, zawierający funkcje: antywirusa, *firewall'a*, *antyspyware*, *antyspam*, moduł chroniący prywatne dane – *Privacy Control* oraz moduł kontroli rodzicielskiej – *Parental Control*. Jedną z nowości w aktualnej wersji programu jest funkcja *QuickScan*, której zadaniem jest szybkie skanowanie systemu po każdej aktualizacji bądź wirusów. Z nowymi typami zagrożeń internetowych jest także związany jego moduł – *Worm Protection*, która sprawdza, czy nasz komputer jest chroniony przed najbardziej złośliwymi wirusami – tzw. „robakami sieciowymi". Program posiada wszystkie najważniejsze cechy pakietu kompleksowej ochrony komputera podłączonego do sieci Internet, a jego praca charakteryzuje się dużą stabilnością i szybkością skanowania plików. Jednak program posiada jedną wadę, która może być nie do zaakceptowania dla posiadaczy wolniejszych

Programy antyspyware					
Program	Ad-Aware SE Personal Edition	Ad-Aware SE Personal	Spybot - Search & Destroy	Microsoft AntiSpyware	PestPatrol
Cena	freeware do użytku domowego	39.95 USD	freeware	freeware	30 USD
Wersja	1.06	1.06r1	1.4	Beta 1	2005
WWW [http://]	www.lavasoft.com/	www.lavasoft.com/	www.safer-networking.org/	www.microsoft.com/athome/security/spyware/software/default.mspx	www.ca.com/products/pestpatrol/
Ochrona w czasie rzeczywistym - rezydent	nie	tak	tak	tak	tak
Przywracanie skasowanych plików	tak	tak	tak	tak	tak
Własny harmonogram skanowania	nie	tak	tak	tak	tak
Polska wersja	nie	nie	tak	nie	nie

komputerów – dość mocno obciąża system, a czas otwierania poszczególnych programów zwiększa się, gdy jest włączona funkcja „Auto-Protect".

Bardzo ciekawym rozwiązaniem jest program **Kaspersky Personal Security Suite**, który również jest rozwiązaniem kompleksowym, lecz znacznie mniej obciąża system operacyjny, niż wspomniane oprogramowanie firmy Symantec. Program jest bardzo prosty w użyciu, posiada intuicyjne menu, a więc dopasowanie parametrów ochrony do indywidualnych potrzeb nie powinno nikomu sprawiać problemów. Wart dodać, iż w niektórych testach program uzyskał aż 99-procentową skuteczność wykrywania wirusów (na specjalnie przygotowanym zestawie wirusów), co jest wynikiem wręcz rewelacyjnym. Program domyślnie nie skanuje plików skompresowanych, więc jeśli chcemy, aby te pliki były sprawdzane na obecność wirusów musimy taką opcje ustawić sami.

Stosunkowo niedrogim, a zarazem bardzo skutecznym rozwiązaniem jest program **BitDefender 9 Internet Security**, który proponuje wszystkie typy ochrony jakie potrzebuje użytkownik korzystający z Internetu. Dostarcza niezbędną ochronę przed wirusami, *spywarem*, *spamem*, *phishingiem*, intruzami i niepożądaną zawartością stron WWW. Używa wydajnych silników skanujących certyfikowanych między innymi przez ICSA Labs, Virus Bulletin, Checkmark i TÜV. Jego moduł *firewall* filtruje przychodzący i wychodzący ruch sieciowy, kontroluje pliki cookie, a także blokuje złośliwe skrypty i dialery. W trybie *Stealth* komputer jest „niewidoczny" dla złośliwego oprogramowania i hakerów. Program oparty jest na nowoczesnej technologii *Heurestic in Virtual Enviroment* (HIVE), która emuluje „wirtualny komputer wewnątrz danego komputera", gdzie fragmenty podejrzanego oprogramowania są uruchamiane, aby sprawdzić czy nie mają złośliwego zachowania. Ma to znaczenie szczególnie w przypadku, gdy nasz system zostanie zainfekowany nowym, nieznanym dotychczas wirusem.

Innym rozwiązaniem, które stosunkowo niedawno pojawiło się na rynku polskim jest pakiet **F-Secure Internet Security 2006** fińskiej firmy F-Secure. Składa się ze ściśle zintegrowanych ze sobą systemów ochrony antywirusowej, osobistej zapory ogniowej, systemu *intrusion detection*, *antyspam*, *antispyware* oraz kontroli aplikacji z dostępem do Internetu, a więc jest typowym przykładem całkowitej ochrony komputera. Kilka mechanizmów skanowania gwarantuje pełną ochronę także przeciwko nowym, nieznanym wirusom. Aby ułatwić instalację, oprogramowanie przeszukuje system i usuwa inne zainstalowane aplikacje antywirusowe, które potencjalnie mogą powodować konflikty i w efekcie niestabilność działania systemu. To na co warto zmówić uwagę w przypadku tego pakietu, to fakt, iż baza definicji wirusów jest automatycznie i w sposób niewidoczny dla użytkownika aktualizowana 1–2 razy dziennie przy minimalnym obciążeniu sieci. Definicje te są ponadto podpisane cyfrowo, co zapewnia ich autentyczność. Moduł *Antispyware* chroni system przed instalowanymi bez wiedzy użytkownika aplikacjami szpiegującymi, a samo oprogramowanie bazuje na produkcie Ad-Aware firmy Lavasoft.

Warto rozważyć także zakup rodzimego pakietu typu *Internet Security* – programu **mks_vir 2005.** Kultowy, już można powiedzieć, polski program antywirusowy nie tak dawno został wyposażony w moduł zapory ogniowej (*firewall*). W jego skład wchodzi także specjalny monitor nadzorujący korzystanie przez inne aplikacje z najbardziej wrażliwych punktów rejestru systemowego Windows.

Z programów zawartych w tabeli warto zwrócić uwagę na specyficzne funkcje pakietu **McAffe Internet Security**, który potrafi wykrywać próby infekcji podczas synchronizacji danych, np. komputera stacjonarnego z notebookiem, a specjalny moduł *ScriptStopper* monitoruje podejrzane wykonania skryptów oraz powstrzymuje wirusy i robaki internetowe przed przenoszeniem się poprzez pocztę elektroniczną na inne komputery.

Dodatkowy program *antispyware* to dodatkowe zabezpieczenie

Programów *antyspyware* na rynku jest całe mnóstwo, problem jest jednak w tym, aby wybrać spośród tych najlepszych, które rzeczywiście ochronią nasz system przez programami szpiegowskimi. Warto wiedzieć także, że większość tego typu programów zamiast chronić przez tym złośliwym oprogramowaniem, pomaga się im rozprzestrzeniać! Jednym z najlepszych rozwiązań są tak naprawdę 3 programy: **Ad-Aware SE** (w wersji Personal – bezpłatnej, oraz w wersji Pro, za którą trzeba zapłacić), oraz programy **PestPatrol** (również wersja komercyjna) i darmowy, lecz niezwykle skuteczny **Spybot – Search & Destroy**. Warto wiedzieć, że programy te mogą być zainstalowane bez względu na to, czy nasz pakiet *Internet Security* posiada wbudowany moduł *antispyware*. Wszystkie te 3 programy wyposażone są w moduł rezydentny (Ad-Aware SE, niestety tylko w wersji Pro), którego zadaniem jest skanowanie w czasie rzeczywistym systemu na obecność programów szpiegowskich i innej maści robaków. Używanie tych programów wzmocni dodatkowo ochronę naszego komputera przez złośliwym oprogramowaniem.