

Jak chronić komputer przed złośliwym oprogramowaniem i spamem

Nigdy więcej spamu!

Kiedy rano włączam mój komputer, mam wrażenie, że moja skrzynka pocztowa to cel ataku wszystkich internetowych przestępców. Wciąż upewniam się, że Internet jest pełen hakerów, wirusów, koni trojańskich i złośliwych programów.

PATRICIA JUNG

Czy to dobry pomysł, aby korzystać z komputera podłączonego do pełnego zagrożeń Internetu? Tak jak w życiu normalnym, odpowiedź brzmi „tak” – o ile posiadamy odpowiednią wiedzę i korzystamy ze stosownych środków ochrony. Jednak nawet wówczas nie można mieć stu-procentowej pewności, że nie zostaniemy znienacka zaatakowani.

Przecież i w życiu codziennym można utopić się w wannie, większość ludzi czuje się też wystarczająco bezpiecznie opuszczając swoje mieszkania i spacerując po ulicach, chociaż statystycznie rzecz biorąc, na ulicy są bardziej narażeni na złodziei, nieuważnych kierowców czy zabójców. Sytuacja w świecie wirtualnym jest podobna. Jeśli odwiedzasz strony WWW, istnieje niebezpieczeństwo infekcji złośliwym oprogramowaniem; jeśli korzystasz z poczty elektronicznej, wcześniej czy później zostaniesz zaatakowany przez spamerów, i wreszcie, jeśli Twój komputer jest podłączony do Internetu – może zostać zaatakowany przez hakerów.

Co więcej, nie ma powodów i coraz częściej możliwości, aby zrezygnować z korzystania

z Internetu – korzyści przeważają ryzyko. Nie ma sensu chować głowy w piasek, zamiast tego najlepiej zacząć pracę nad rozwojem technik, które zapewnią jak największą ochronę przed zagrożeniami.

W przypadku wirusów, koni trojańskich i robaków, używanie Linuksa jest najlepszym sposobem na zabezpieczenie się przed nimi. Z jednej strony Linux jako system operacyjny zapewnia odpowiedni stopień ochrony – przy założeniu, że korzystając z Internetu używamy nieuprzywilejowanego konta. Z drugiej strony Linux i aplikacje dla niego przeznaczone nie są zbyt atrakcyjnym celem dla twórców złośliwego oprogramowania (przynajmniej do tej pory tak było). Nasze artykuły pokażą, jakie środki zabezpieczające są najbardziej skuteczne wobec tych zagrożeń.

Odporny, ale nie bierny

Mimo że wirusy dla Windows nie mogą

atakować oprogramowania linuksowego, odpowiedzialny internauta będzie starał się nie narażać użytkowników Windows na ewentualne wirusy rozpowszechniane za pośrednictwem swojego komputera. Jest na to wiele sposobów: regularne skanowanie plików na serwerach dostępnych dla użytkowników Windows (np. Samba; sprawdzanie wiadomości e-mail przed wysłaniem do użytkownika Windows itd.).

Na końcu zajmiemy się spamem, dotyczącym wszystkich użytkowników Internetu. Pojedyncie aktywne jest trudne do realizacji, jeśli nie jesteśmy administratorem serwera pocztowego, ale również zwykli użytkownicy mają pewne możliwości. Przedstawimy także techniki, które sprawiają, że Twój adres e-mail zostanie ukryty dla spamerów tak długo, jak to tylko możliwe. Pokażemy też, jak kontrolować wiadomości na serwerze POP3, zanim zostaną ściągnięte przez program pocztowy. ■

Cover Story

Strony WWW odporne na spam18

Jak projektować i tworzyć serwisy WWW odporne na spam. Jak walczyć ze spamerami, którzy używają automatycznych narzędzi do zbierania adresów e-mail ze stron WWW.

Anty-spam na POP322

Jak zaoszczędzić miejsce na dysku, usuwając spam bezpośrednio na serwerze POP3, zanim zostanie pobrany przez program pocztowy.

Antywirus26

Walczymy z wirusami dla Windows z poziomu Linuksa, zabezpieczając całą sieć lokalną przy pomocy programu antywirusowego ClamAV.

