

Zapobieganie obecności szkodliwych programów w systemie komputera to ciągły proces przeciwdziałania hakerskim atakom. Aktualizacje systemu oraz programy antywirusowe minimalizują ryzyko infekcji jednak użytkownicy komputerów wyrabiając prawidłowe nawyki podczas surfowania w sieci powinni pamiętać o zachowaniu ostrożności oraz rozsądku.

1. **Aktualizacje i łatanie dziur systemowych** - Podstawową zasadą zachowania bezpieczeństwa są aktualizacje systemu oraz innych aplikacji zainstalowanych w komputerze. Niestety szerokie grono użytkowników nie stosuje się do tych podstawowych zaleceń, a przyczyną braku instalacji poprawek prawdopodobnie są pirackie kopie programów użytkowych lub SO Windows. Łukasz Nowatkowski G Data Software: „... ze względu na dużą popularność nielegalnych kopii systemów Windows oraz innych pirackich programów użytkowych, ich właściciele nie stosują się do pierwszego kroku mającego na celu łatanie dziur w oprogramowaniu. Aktualizacje stanowią podstawę ochrony przed wirusami i zapobiegają powstaniu globalnej infekcji.” Brak dbałości o aktualizację systemu wśród nielegalnych użytkowników z pewnością związany jest z obawami ujawnienia ich tożsamości oraz w wybranych przypadkach blokady dostępu do aktualizacji.

2. **Program antywirusowy** - Proces aktualizacji stanowi również podstawę do efektywnego działania programów antywirusowych. Obecnie absolutną koniecznością jest stosowanie tego typu oprogramowania ochronnego. Komercyjne pakiety takie jak G Data Software, Kaspersky lub darmowe wersje programów np.: Avast czy Avira Free przede wszystkim wymagają aktualizacji baz sygnatur wirusów. Niektórzy eksperci twierdzą, że tylko przeprowadzanie codziennych aktualizacji programów antywirusowych jest skuteczne.

3. **Dodatkowy moduł AntiSpyware** - Kolejnym krokiem do bezpiecznego surfowania jest wyposażenie komputera w moduł AntiSpyware, umożliwiający wyszukiwanie złośliwego oprogramowania szpiegującego. Szkodniki typu Spyware zawierają mechanizmy monitorujące Twoje nawyki podczas pracy z komputerem i w Internecie. Dzięki nim szpieg dowie się jakie strony www otwierasz najczęściej, czym się interesujesz i kiedy korzystasz z komputera. Większość programów antywirusowych znanych producentów zawiera moduł AntiSpyware.

4. **Firewall** – To narzędzie pozwalające zarządzać dostępem wybranych programów do sieci. Firewall monitoruje działanie programów i w razie próby niekontrolowanego kontaktu aplikacji z Internetem reaguje. Dzięki niemu każda próba wysłania wykradzionych przez hakera danych będzie niemożliwa. Firewall może być częścią pakietu antywirusowego lub niektórych urządzeń takich jak routery i modemy.

5. **Mocne Hasło** – Słabe hasło nie stanowi żadnego zabezpieczenia przed dostępem cyberprzestępcy do konta użytkownika. Hakerzy od dawna potrafią szybko łamać proste hasła. Aby zapewnić maksimum bezpieczeństwa np. swojej skrzynki e-mail lub konta na naszej-klasie, konieczne jest zastosowanie niestandardowych słów np. z dodatkiem znaków specjalnych lub dowolnego łańcucha np. L!Omtjjz1. Dla zapamiętania tak trudnego hasła można posłużyć się metodą pierwszych liter ulubionego tekstu piosenki lub wiersza. Układając powyższe hasło posłużyłem się znaną wszystkim Polakom inwokacją „Litwo Ojczyzno moja! Ty jesteś jak zdrowie”, przy czym 1 oznacza pierwszą księgę Pana Tadeusza. Używanie różnych haseł dostępu do kont w sieci lub aplikacji daje dodatkową warstwę ochrony przed atakiem.

6. **Zasada ograniczonego zaufania** – Stosując powyższe metody ochrony komputera dodatkowo musimy pamiętać o zasadzie ograniczonego zaufania do pozostałych użytkowników sieci Internet. Otrzymując wiadomości, w których zawarte są linki lub załączniki nie otwierajmy ich zbyt pochopnie. Tego typu linki mogą prowadzić do groźnych witryn, których zadaniem jest wyłudzenie danych personalnych lub innych ważnych prywatnych informacji. Surfując w sieci lub korzystając z usług on-line zachowujmy czujność i nie dajmy się omamić gorącymi ofertami, imitacją strony banku, czy też fałszywym alarmem nakłaniającym do ściągnięcia pliku z prawdziwym wirusem.

Jeśli Twój system jest już zainfekowany i komputer zmienił się w zombie możesz uruchomić program do usuwania

wirusów i próbować zerwać połączenie między komputerem, a atakującym. Niestety bywają przypadki, że jedynym sposobem usunięcia szkodnika jest rozpoczęcie instalacji od zera. Dlatego na wszelki wypadek tak ważna są regularne kopie zapasowe twardego dysku. Dodatkowo w celu wykluczenia uszkodzeń plików pamiętaj o skontrolowaniu programem antywirusowym pozostałych plików na dysku.

Źródło: **G Data Software**