

Profilaktyka

Obrona bierna nie polega ona na bezpośredniej walce z wirusami, lecz na maksymalnym ograniczeniu skutków ich działania.

Użycie programów antywirusowych to druga metoda ochrony naszego komputera – obrona czynna.

Pierwsza metoda to specjalne programy dołączające do systemu operacyjnego i śledzące aktywność uruchamianych na komputerze programów.

Metoda druga to programy obliczające sumy kontrolne wszystkich dostępnych na dyskach programów i zapisujące je w specjalnym zbiorze. Przy kolejnym uruchomieniu sprawdzają one, czy któryś z programów nie został zmodyfikowany. Jeżeli tak się stało to użytkownik jest o tym sygnalizowany. Jedną z poważniejszych wad tego typu programów jest ich nieskuteczność w nowych już zainfekowanych programach.

Trzeci sposób to programy polujące na określone typy wirusów, na ogół dość szybkie i potrafiące unieszkodliwiać je bez niszczenia programu będącego nosicielem wirusa.

Obrona przed szkodliwym oprogramowaniem:

- włączenie aktualizacji automatycznej systemu,
- instalacja oprogramowania antywirusowego, włączona zaporą sieciową (firewall),
- aktualizacja oprogramowania,
- zaktualizowany program i bazy,
- włączone automatyczne aktualizacje programu i baz,
- włączenie monitora (korzystanie z funkcji),
- nie otwieranie załączników poczty elektronicznej niewiadomego pochodzenia,
- czytanie okien instalacyjnych aplikacji,
- wyłączanie makr w plikach MS Office nieznanego pochodzenia,
- regularne całosciowe skanowanie systemu programem antywirusowym,
- przy płatnościach drogą elektroniczną upewnienie się że transmisja danych będzie szyfrowana,
- używanie oryginalnego systemu i aplikacji, pochodzących z legalnego źródła,

- właściwa konfiguracja przeglądarki programów pracujących w sieciach np. Internecie.

korzystać z:

- programów usuwających adware oraz spyware, które mogły nie zostać wykryte przez program antywirusowy lub na których instalację użytkownik zgodził się nieświadomie,
- dodatków blokujących reklamy - doskonale sprawdzają się takie jak: Adblock, Adblock Plus,
- programów do wykonywania kopii zapasowych najważniejszych plików lub całych dysków
- możliwości przechowywania plików online, w tak zwanej „chmurze”,

dodatkowo:

- uważnie czytać komunikaty, które pojawiają się w czasie instalacji programów,
- świadome odpowiadanie na komunikaty systemu.
- pobierać programy i aplikacje jedynie z zaufanych stron internetowych,
- regularnie aktualizować zainstalowane oprogramowanie, a przede wszystkim system operacyjny,
- regularnie skanować dyski programem antywirusowym,
- nie otwierać załączników wiadomości e-mail od nieznanych nadawców,
- nie klikać w pojawiające się reklamy i informacje o wygranych,
- praca na koncie z ograniczeniami,
- używanie konta administrator tylko w niezbędnych sytuacjach
- stosowanie bezpiecznych haseł,
- administrowanie (za pomocą run as) z konta z ograniczeniami za pomocą metody uruchom jako,
- instalowanie firmowego (licencjonowanego) oprogramowania,
- instalowanie aktualnych poprawek (SP i hotfixy) dla systemu i oprogramowania,
- cykliczne analizowanie bezpieczeństwa systemu np.: korzystanie z oprogramowania do wykrywania luk w bezpieczeństwie systemu,
- systematyczne sprawdzanie stanu pamięci operacyjnej, dysków i plików za pomocą programów do usuwania szkodliwego kodu np.: antywirusowego,

- zabezpieczanie nośników (mechaniczne i programowe, np.: dyskietek przed zapisem),
- ostrożność przy rejestrowaniu się i pracy na obcych terminalach,
- nie pobierać nieznanych plików,
- wykonywanie kopii systemu i danych

Nie ma zasad, gwarantujących bezwirusową pracę. Istnieją jednak reguły, pozwalające zminimalizować ryzyko zarażenia, a w razie infekcji zmniejszające skutki działań niszczących wirusa.