Załącznik nr 6
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu Wojewódzkiego

Instrukcja w zakresie profilaktyki antywirusowej

Metody i działania związane z profilaktyką antywirusową w systemach informatycznych użytkowanych w sieci komputerowej Urzędu.

Osobą prowadzącą działania profilaktyczne mające na celu ochronę zasobów sieci komputerowej Urzędu przed atakami wirusów komputerowych jest administrator systemu.

1. Administrator systemu wykorzystuje następujące funkcje systemowe:
   a) rejestracja i śledzenie informacji o dostępach lub próbach dostępu do zasobów i usług danego systemu.
   b) rejestracja i śledzenie komunikatów o błędach w pracy systemu.
   c) szyfrowanie i uwierzytelnianie informacji przesyłanych w sieci.
   d) wykrywanie obecności fałszywego oprogramowania w danych wpływających do systemu z sieci Internet.
   e) kontrola integralności oprogramowania zainstalowanego w systemie.

2. Ochrona antywirusowa zasobów informatycznych jest realizowana przez system antywirusowy posiadający następujące funkcje:

   a) zabezpieczenie zasobów informatycznych przed wirusami komputerowymi za pomocą modułu rezydentnego, skanującego na bieżąco wszystkie zasoby komputera,
   b) aktualizację baz sygnatur wirusów na bieżąco,
   c) możliwość automatycznego podejmowania działań w przypadku pojawienia się nowych, nieznanych wirusów (np.: zablokowanie komunikacji z zawirusowanym komputerem).

3. Aktualizacja baz sygnatur wirusów

a) Bazy sygnatur wirusów dla serwerów są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
b) Bazy sygnatur wirusów dla stanowisk roboczych są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
c) Aktualizacja baz sygnatur wirusów odbywa się nie rzadziej niż jeden raz każdego dnia roboczego.

4. Kontrola antywirusowa.

a) Zasoby informatyczne są skanowane na bieżąco za pomocą modułu rezydentnego. Kontroli podlegają wszystkie pliki (odczytywane i zapisywane) w tym poczta elektroniczna;
b) System antywirusowy jest zaprogramowany do wykonywania okresowych kontroli antywirusowych całego systemu plików. Kontrole te są wykonywane przez program automatycznie nie rzadziej niż jeden raz w tygodniu;
c) Zabrania się korzystania ze stanowiska bez aktywnego programu antywirusowego.

Zalecenia dla użytkowników stacji roboczych.

1. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (czytniki DVD, porty USB itp.) nośników rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi itp.
2. Zabrania się bez zgody Wydziału Organizacji i Kadr używania na stanowisku pracy urządzeń do gromadzenia i przenoszenia danych, takich jak pamięci „flash" dołączane przez porty USB, karty radiowe, urządzenia „bluetooth", dyski wymienne, modemy nie będących własnością Urzędu.
3. Zabrania się wykorzystywania do celów służbowych bez zgody Wydziału Organizacji i Kadr innych, niż dopuszczony w ŚUW, systemów poczty elektronicznej.

4. Z uwagi na próby ataków na systemy użytkowników poprzez zainfekowanie poczty elektronicznej zaleca się zachowanie szczególnej ostrożności przy otwieraniu otrzymanych tą drogą załączników. W przypadku otrzymania nieoczekiwanej przesyłki pocztowej, która zawiera załącznik lub odsyła do treści bezpośrednio do strony www zaleca się aby nie otwierać załącznika ani nie korzystać bezpośrednio z przesłanych odnośników.

5. Zaleca się wyłączenie opcji autopodglądu załącznika w programie pocztowym Outlook.

6. Korzystając z programów MS Office (Word, Excel itp.) i podobnych należy, jeśli to możliwe, uaktywnić ich wewnętrzny system ochrony przed wirusami MAKRO.

7. Należy systematycznie przeprowadzać kontrolę antywirusową stanowiska programem dostarczonym przez Wydział Organizacji i Kadr.

8. Każdy nośnik danych, używany do przenoszenia danych pomiędzy stanowiskami komputerowymi, przed odczytaniem danych należy sprawdzić programem antywirusowym.

Postępowanie w przypadku ujawnienia lub podejrzenia istnienia wirusa:

1. Gdy zachowanie systemu komputerowego odbiega od normy (komunikaty o błędach, nieoczekiwane zniknięcie lub pojawienie się plików lub katalogów, spowolniona praca systemu, dziwne lub niezrozumiałe informacje pojawiające się na ekranie itp.) należy również przeprowadzić kontrolę antywirusową systemu.

2. Jeśli program antywirusowy stwierdził istnienie wirusa na nośniku danych taki nośnik należy natychmiast wyjąć z czytnika (stacji dyskietek, czytnika DVD,USB itp.), wyraźnie oznaczyć i przekazać nośnik administratorowi systemu. Następnie należy sporządzić notatkę służbową ze zdarzenia i przeprowadzić kontrolę antywirusową całego systemu.

3. Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy należy niezwłocznie zgłosić ten fakt do Oddziału ds. Informatyki pod numer telefonu 17-52. Zabrania się samodzielnego usuwania zainfekowanych plików.

4. Użytkownik ma obowiązek zgłaszania do WOiK wszelkich zauważonych niestandardowych zachowań systemu antywirusowego.