7 Zabezpieczanie systemu operacyjnego

ZAGADNIENIA

- **W jaki sposób działają wirusy komputerowe?**
- **Jak chronić system przed zawirusowaniem?**
- **W jaki sposób zainstalować i skonfigurować program antywirusowy?**
- **W jakim celu należy używać zapór ogniowych i włączać aktualizacje systemu?**
- **Jak skonfigurować zaporę sieciową w systemach Windows i Linux?**

Zabezpieczenie systemu operacyjnego to przede wszystkim:
- stała aktualizacja systemu operacyjnego;
- dobry program antywirusowy;
- prawidłowa konfiguracja zapory firewall;
- przestrzeganie polityki bezpieczeństwa.

7.1. Rodzaje wirusów komputerowych

Wirusy komputerowe to programy tworzone specjalnie do zakłócania pracy komputera, rejestrowania, uszkadzania, usuwania danych albo rozprzestrzeniania się do innych komputerów za pomocą sieci internet, często w celu spowolnienia pracy systemu. Podobnie jak wirusy atakujące człowieka różnią się zjadliwością, wirusy komputerowe mogą być tylko lekko irytujące, ale niekiedy są destrukcyjne. Mogą przybierać ponadto nowe i różnorodne postaci. Dobrą wiadomością jest to, że – przy odrobinie wiedzy i zapobiegliwości – można zmniejszyć prawdopodobieństwo stania się ofiarą wirusów i ograniczyć skutki ich działania.

Rodzaje wirusów komputerowych:
- wirusy pasożytnicze,
- wirusy towarzyszące,
- wirusy plików wsadowych,
- makrowirusy,
- generatory wirusów,
- robaki,
- konie trojańskie,
- bomby logiczne,
- keyloggery.

Wirusy wykorzystują słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i beztroskę użytkowników.

Często wirusami komputerowymi mylnie nazywane są wszystkie złośliwe programy. Do zwalczania wirusów, usuwania ich i zabezpieczania się przed nimi używa się programów antywirusowych.

7.2. Zasady działania wirusów komputerowych

Wirusy zwykle wymagają, aby nieostrożny użytkownik komputera nieświadomie je przekazał lub wysłał. Niektóre bardziej wyrafinowane wirusy mogą się samodzielnie powielać i wysyłać do innych komputerów przez przejęcie kontroli nad innymi programami, takimi jak aplikacja do obsługi poczty elektronicznej.

Konie trojańskie (od mitycznego konia trojańskiego) to szkodliwe oprogramowania, które m.in. umożliwiają kontrolowanie komputera przez sieć komputerową. Mogą wyglądać na użyteczne programy, co ma na celu nakłonienie użytkownika do ich pobrania. Niektóre konie trojańskie mogą nawet dawać oczekiwane rezultaty, jednocześnie potajemnie infekując system użytkownika lub inne komputery działające w sieci. Chociaż dobrze jest zdawać sobie sprawę z istnienia różnych rodzajów wirusów i sposobów ich działania, najistotniejsze jest, by regularnie uaktualniać oprogramowanie komputera z wykorzystaniem najnowszych aktualizacji i narzędzi antywirusowych, być na bieżąco w kwestii nowych zagrożeń i przestrzegać kilku podstawowych zasad przy przeglądaniu stron internetowych, pobieraniu plików i otwieraniu załączników. Gdy wirus znajdzie się w komputerze, jego rodzaj czy metoda, jakiej użył, by się tam znaleźć, nie są tak istotne, jak usunięcie go i zapobieżenie dalszej infekcji. W funkcjonowaniu wirusów można wyodrębnić dwie fazy:

1. faza rozmnażania się wirusa – polega na umieszczeniu jego zaszyfrowanego kodu w kolejnych miejscach systemu komputerowego.
2. faza destrukcji – polega na ujawnieniu się wirusa. To, czego wirus w ramach destrukcji (II faza – jawna) dokonuje, jest zależne od umiejętności, wiedzy, fantazji i złośliwości jego twórcy.

Wirus może dołączyć się do nosiciela na trzy sposoby:

1. Dołączając się na końcu nosiciela (nosiciel => wirus).
2. Dołączając się na początku nosiciela (wirus => nosiciel).
3. Dołączając się na końcu i na początku nosiciela. Są to najgroźniejsze wirusy typu SHELL, które wtapiają w nosiciela swój kod (wirus => nosiciel => wirus).

Różnica w działaniu wirusów z tych trzech grup polega na tym, że w pierwszym wypadku wirus replikuje się i zaraża inne pliki po zakończeniu działania programu, jakim jest nosiciel. W drugim wypadku najpierw replikuje się wirus, a następnie dochodzi do wykonania programu nosiciela. W trzecim wypadku spełnione są oba warunki.

7.3. Objawy zainfekowania komputera wirusem

Po otwarciu i uruchomieniu zainfekowanego programu lub załącznika na komputerze użytkownik może nie zdawać sobie sprawy, że wprowadził wirus, dopóki nie zauważy nietypowego zachowania komputera. Oto kilka podstawowych objawów wskazujących na możliwość zainfekowania systemu:

- komputer pracuje dużo wolniej niż zwykle;
- często przestaje reagować na polecenia lub się zawiesza;
- co kilka minut przestaje działać i uruchamia się ponownie,
- samodzielnie uruchamia się ponownie, po czym nie działa w normalny sposób;
- aplikacje nie działają prawidłowo;
- dyski lub napędy są niedostępne;

- drukowanie nie działa prawidłowo,
- wyświetlane są niespotykane komunikaty o błędach;
- menu i okna dialogowe są zniekształcone.

Są to często spotykane oznaki infekcji, lecz mogą one również wskazywać na problemy ze sprzętem lub oprogramowaniem, które nie mają nic wspólnego z wirusem. Jedną z najskuteczniejszych metod zabezpieczenia komputera przed zainfekowaniem wirusami jest zainstalowanie aktualnego i skutecznego oprogramowania antywirusowego.

7.4. Usuwanie wirusów

Nawet dla eksperta skuteczne usunięcie wirusa z komputera bez pomocy określonych narzędzi do tego przeznaczonych stanowi często nie lada wyzwanie. Niektóre wirusy i inne niepożądane programy są tak zaprojektowane, że po ich wykryciu i usunięciu instalują się ponownie. Na szczęście regularne aktualizowanie komputera i korzystanie z narzędzi antywirusowych oferowanych przez wiele firm może pomóc trwale usunąć niepożądane oprogramowanie (i zapobiegać ponownej jego instalacji).

Ze względu na to, że żadna metoda nie gwarantuje stuprocentowego bezpieczeństwa, istotne jest regularne tworzenie kopii zapasowej ważnych dla nas plików przed wystąpieniem wirusa lub innych problemów.

Można jednak zwiększyć bezpieczeństwo komputera i ograniczyć możliwość infekcji przez regularne aktualizowanie oprogramowania, utrzymywanie subskrypcji aktualnego oprogramowania antywirusowego i przestrzeganie następujących zasad:

- Regularnie aktualizuj oprogramowanie komputera za pomocą najnowszych aktualizacji, włącz automatyczne aktualizacje.
- Używaj zapory internetowej.
- Wykup subskrypcję oprogramowania antywirusowego znanego producenta i regularnie je aktualizuj.
- Nigdy nie otwieraj załączników e-mail od nieznanych osób.
- Unikaj otwierania załączników e-mail w wiadomościach pochodzących od osób znanych, o ile nie wiesz dokładnie, co załącznik zawiera. Nadawca może nie wiedzieć, że załącznik zawiera wirus.
- Jeżeli korzystasz z aplikacji pakietu Microsoft Office, regularnie je aktualizuj.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Czym są i jakie szkody wyrządzają w komputerze konie trojańskie i robaki?
2. Co to jest spam i jak można się przed nim chronić?
3. Co to są dialery, jakie jest ich działanie? Kto staje się ich ofiarą?
4. Jaką nazwę nosi proceder pozyskiwania poufnych danych przez podszywanie się pod osobę, której te informacje są rzekomo potrzebne?

7.5. Instalacja i konfiguracja programów antywirusowych i antyspyware

Aby mieć pewność, że komputer jest prawidłowo zabezpieczony przed wirusami, należy przeprowadzać na bieżąco wszelkie dostępne aktualizacje systemu operacyjnego i mieć oprogramowanie antywirusowe.

Program antywirusowy to dzisiaj bardzo ważny składnik każdego komputera podłączonego do globalnej sieci, i nie tylko. Internet poza wieloma korzyściami niesie także liczne

zagrożenia w postaci wszelkiego rodzaju niechcianego oprogramowania, które może zainfekować nasz system oraz narazić na utratę ważnych danych.

Program antywirusowy (antywirus) to program komputerowy, którego celem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych.

Współcześnie najczęściej jest to pakiet programów chroniących komputer przed różnego typu zagrożeniami.

Programy antywirusowe często są wyposażone w dwa niezależnie pracujące moduły:

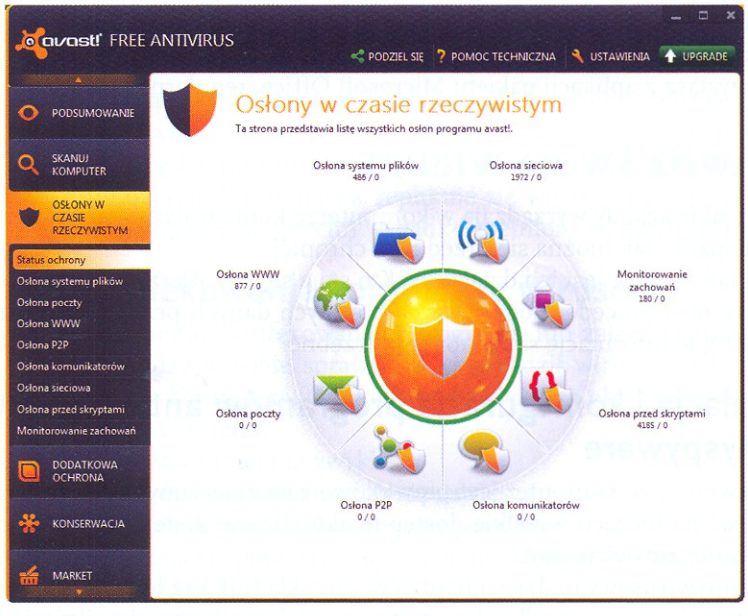
- **skaner**, który bada pliki na żądanie lub co jakiś czas; służy do przeszukiwania zawartości dysku;
- **monitor**, który bada pliki w sposób automatyczny; służy do kontroli bieżących operacji komputera.

Program antywirusowy powinien również mieć możliwość aktualizacji definicji nowo odkrytych wirusów, najlepiej na bieżąco, przez pobranie ich z internetu, ponieważ dla niektórych systemów operacyjnych codziennie pojawia się około trzydziestu nowych wirusów. Przykładem zupełnie darmowego programu antywirusowego dla użytkowników domowych jest Avast! Instalacja oraz konfiguracja jest bardzo prosta i wymaga niewielkiej interakcji użytkownika.

PRZYKŁAD 7.1

Instalacja i konfiguracja programu antywirusowego na przykładzie programu Avast!

1. Ściągnij plik instalacyjny ze strony np. `http://www.avast.com/pl` i zapisz.
2. Następnie kliknij na nim prawym przyciskiem myszy i z menu podręcznego wybierz opcję **`Uruchom jako administrator`**.
3. W kolejnym oknie możesz wybrać rodzaj instalacji – np. **`Instalacja ekspresowa`**.
4. Po wybraniu rodzaju instalacji rozpoczyna się proces instalacyjny, który trwa kilka minut.



Rys. 7.1. Konfiguracja programu antywirusowego

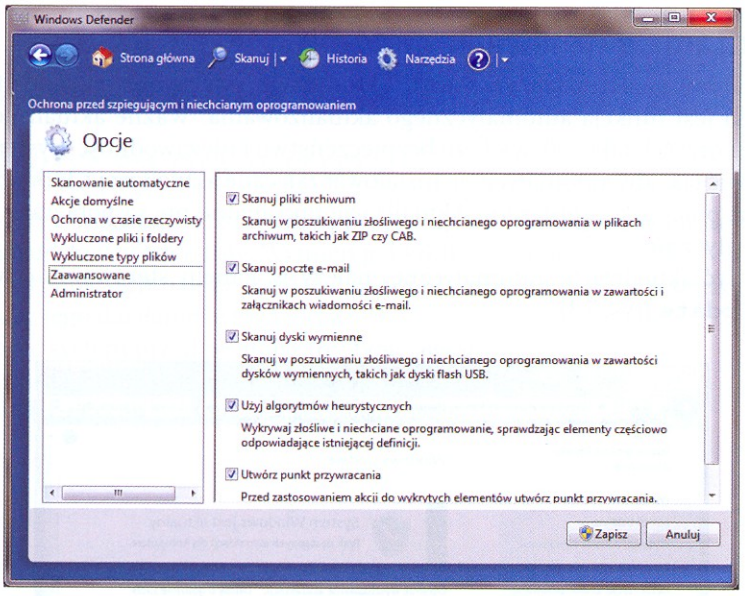
5. Przed końcem procesu instalacji program Avast! przeprowadza szybkie skanowanie komputera.
6. W ostatnim kroku należy dokonać bezpłatnej rejestracji.

Konfigurację programu możemy wykonać, klikając na nim prawym przyciskiem myszy i wybierając z menu podręcznego opcję: **Otwórz interfejs użytkownika programu Avast!**. Z lewej strony okna programu możemy wybrać ochronę i dostosować ją do własnych potrzeb (rys. 7.1).

Programy szpiegujące (*spyware*) to programy komputerowe, których celem jest szpiegowanie działań użytkownika. Programy te gromadzą informacje o użytkowniku i wysyłają je często bez jego wiedzy i zgody autorowi programu. Do takich informacji należą między innymi:

- adresy stron internetowych odwiedzanych przez użytkownika,
- dane osobowe,
- numery kart płatniczych,
- hasła,
- adresy poczty elektronicznej.

Programy tego typu zaliczane są do kategorii złośliwego oprogramowania. Obecnie funkcjonują one niemal wyłącznie w środowisku Microsoft Windows. Do wykrywania, usuwania i zwalczania tego typu programów służą programy antyspyware, np.: **Spybot Search & Destroy**, **Windows Defender**.



Rys. 7.2. Konfiguracja Windows Defender

Usługa **Windows Defender** jest oprogramowaniem antyszpiegowskim dołączonym do systemu Windows 7 i uruchamianym automatycznie po włączeniu systemu. Usługa ta oferuje dwa sposoby ochrony komputera przed zainfekowaniem programami szpiegującymi:

- **Ochrona w czasie rzeczywistym** – alarmuje użytkownika w przypadku próby zainstalowania lub uruchomienia programu szpiegującego na komputerze;

- **Opcje skanowania** – możliwość skanowania komputera w poszukiwaniu programów szpiegujących, które mogły zostać zainstalowane na komputerze. Można także ustalać harmonogram regularnego skanowania i automatycznie usuwać dowolne elementy wykryte podczas skanowania. W czasie korzystania z usługi **Windows Defender** należy regularnie aktualizować jej definicje. Usługa **Windows Defender** korzysta z tych definicji w celu zaalarmowania użytkownika o potencjalnych zagrożeniach, gdy ustali, że wykryte oprogramowanie to program szpiegujący lub inne niechciane oprogramowanie. W celu ułatwienia procesu aktualizacji definicji usługa **Windows Defender** współpracuje z usługą **Windows Update**, która przeprowadza na bieżąco automatyczną instalację nowych definicji.

Aby dostosować opcję usługi **Windows Defender**, należy otworzyć ją z **Panelu sterowania**, otworzyć zakładkę **Narzędzia** i następnie **Opcje**. W lewym panelu okna (rys. 7.2) możemy dokonać konfiguracji interesujących nas elementów oraz ustalić harmonogram skanowania.

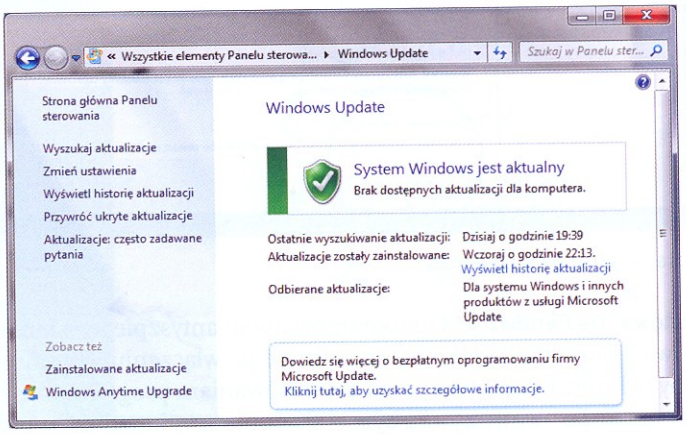
SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyszukaj w internecie i innych źródłach wiedzy informacje o wirusach komputerowych oraz o sposobach ich działania. Wykonaj prezentację multimedialną na ten temat.
2. Znajdź w internecie informacje na temat najnowszych programów antywirusowych i zapoznaj się z ich działaniem. Zainstaluj, jeśli to możliwe, program antywirusowy i przeanalizuj jego działanie.

7.6. Włączanie aktualizacji systemu

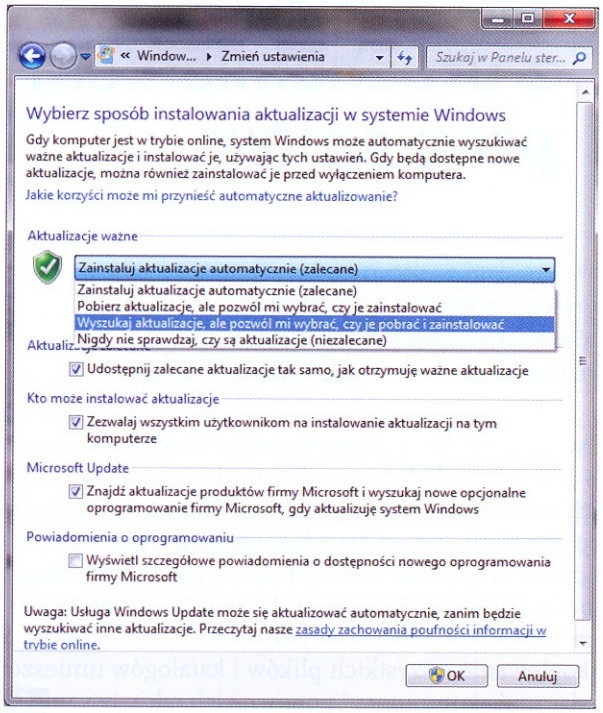
System Windows może instalować ważne aktualizacje, gdy są dostępne, ale tylko wtedy, gdy włączona jest funkcja automatycznego aktualizowania. Ważne aktualizacje niosą ze sobą istotne korzyści, takie jak większe bezpieczeństwo i niezawodność. System Windows można ustawić tak, aby automatycznie instalował zalecane aktualizacje, które mogą zwiększać komfort pracy z komputerem. Aktualizacje opcjonalne nie są pobierane ani instalowane automatycznie.

Aby włączyć aktualizacje automatyczne, należy w Panelu sterowania otworzyć aplet **Windows Update** (rys. 7.3).



Rys. 7.3. Windows Update

Sposób instalowania aktualizacji można wybrać, klikając zakładkę **Zmień ustawienia** (rys. 7.4).



Rys. 7.4. Wybór instalowania aktualizacji

SPRAWDŹ SWOJĄ WIEDZĘ

1. W celu walki z wirusami stosowane są programy antywirusowe. Programy te powinny mieć dwa podstawowe moduły. Wymień je i krótko scharakteryzuj.
2. O jakich czynnościach należy pamiętać podczas codziennej pracy programu antywirusowego, aby jego działanie było efektywne?
3. Jak uchronić system przed programami typu *spyware* i *adware*?
4. Wymień skutki zainfekowania komputera wirusem.
5. Wymień kilka zaleceń profilaktyki antywirusowej.