Marcin Kozłowski

Przed czym i jak chronić komputer?

„Jeśli czegoś nie ma w Google, to znaczy, że nie istnieje" mówi popularny slogan i sporo w nim prawdy. Według szacunkowych danych Google posiada ponad milion serwerów, tak więc ilość danych na nich zgromadzonych jest imponująca. W sieci możemy znaleźć niemal wszystko, np. teksty, grafikę, pliki dźwiękowe, ogromną liczbę stron edukacyjnych oraz różnych programów. Dzięki usługom oferowanym w Internecie dokonujemy przelewów i płatności (bankowość elektroniczna), robimy zakupy w sklepach internetowych i na aukcjach, rezerwujemy bilety lotnicze, zamawiamy bilety do kina czy teatru, rozmawiamy ze znajomymi i nieznajomymi itd. Niestety Internet posiada swoją ciemną stronę z powodu wielu zagrożeń i każdy użytkownik powinien mieć świadomość, jak i przed czym powinien się ochronić.

Złośliwe oprogramowanie (*malware*, *malicious software*) to wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera. Do złośliwego oprogramowania możemy zaliczyć:

- **wirusy komputerowe** – programy bądź fragmenty wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika,
- **robaki** – złośliwe oprogramowanie podobne do wirusów, rozmnażające się poprzez sieć bądź pamięci przenośne; w przeciwieństwie do wirusów robaki są samodzielnymi programami,
- **trojany** – programy udające przydatne oprogramowanie (często posiadające takie funkcje), jednak wykonujące także inne, ukryte przed użytkownikiem działanie; często umożliwiają dostęp do komputera osobom trzecim,
- **rootkity** – bardzo niebezpieczne narzędzie; zasada ich działania polega na ukrywaniu pewnych procesów bądź programów systemowych i pozwalaniu na włamanie do systemu; rootkity są trudne do wykrycia i mogą ukrywać swoją działalność także przed oprogramowaniem antywirusowym,
- **exploity** – kod umieszczany zazwyczaj na stronach internetowych i w aplikacjach (między innymi pliki typu PDF, doc), umożliwiający poprzez luki w oprogramowaniu bezpośrednie włamanie się do komputera ofiary bądź uruchomienie w nim niebezpiecznego programu,
- **keyloggery** – programy służące do odczytywania i zapisania wszystkich naciśnięć klawiszy, przez co cenne informacje mogą dostać się w niepowołane ręce; warto zwrócić uwagę, że *keyloggery* występują także w postaci sprzętowej – zazwyczaj jest to urządzenie podpinane pomiędzy klawiaturą a komputerem,
- **dialery** – programy, których zadaniem jest łączenie się poprzez modem telefoniczny analogowy lub cyfrowy ISDN z płatnymi numerami 0-700 lub z zagranicą; występują głównie na stronach o treściach pornograficznych.

Jak widać klasyfikacja zagrożeń jest bogata. Trzeba mieć także świadomość, że przedstawiony wykaz nie wyczerpuje tematu, a oprócz tego wiele zagrożeń tego typu może posiadać kilka cech – np. koń trojański może być jednocześnie *keyloggerem*. Z tego powodu niezwykle ważna jest profilaktyka antywirusowa. Przede wszystkim ważne jest posiadanie aktualnego oprogramowania antywirusowego z włączoną ochroną w czasie rzeczywistym. Na polskim rynku mamy dość duży wybór oprogramowania antywirusowego, zawsze też może skorzystać z **oprogramowania darmowego, przeznaczonego do użytku osobistego**. Do takich programów należą między innymi:

Avast free antywirus (http://www.avast.com) poza standardowym antywirusem posiada również antyspyware, antyrootkit oraz antymalware. Jest doskonałym zabezpieczeniem antywirusowym zarówno dla typowych komputerów, jak i dużych serwerów. Program posiada polską wersję językową.

AVG Anti-Virus 9.0 Free Edition (http://free.avg.com) zabezpiecza przed wszelakiego rodzaju szkodliwym oprogramowaniem przy zachowaniu niskich wymagań systemowych i częstych aktualizacjach sygnatur wirusów. W jego skład wchodzi skaner główny oraz skaner rezydentny, monitorujący każdy uruchamiany plik, skaner poczty e-mail (współpracujący m.in. z MS Outlook, Outlook

Express), filtr antyspyware, ograniczający dostęp do informacji dla programów szpiegujących i komponentów reklamowych, a także moduł LinkScanner, którego zadaniem jest ochrona przed niebezpiecznym stronami internetowymi, jeszcze przed ich wyświetleniem. Ocenia on również pod kątem bezpieczeństwa wyniki wyszukiwania Google, MSN i Yahoo.

Avira AntiVir Personal (http://www.free-av.com) to program antywirusowy zaprojektowany z myślą o użytku domowym. Zapewnia rozpoznawanie i ochronę przed wirusami, trojanami, programami typu *backdoor*, robakami internetowymi oraz *keyloggerami*, a także ochronę przed nieznanymi wirusami bootsektorowymi, blokując do nich dostęp, gdy tylko pojawi się w nich plik o podejrzanym formacie.

Microsoft Security Essential (http://www.microsoft. com/security_essentials) to bezpłatne narzędzie służące do zabezpieczania systemu Windows przez różnego rodzaju złośliwym oprogramowaniem, takim jak: wirusy, rootkity, trojany i spyware. Program oferuje bardzo przyjazny i prosty w użyciu interfejs graficzny, trzy tryby skanowania (pełne, skrócone i użytkownika, w którym możemy wybrać dyski, a nawet poszczególne foldery), harmonogram skanowania, automatyczne lub definiowane przez użytkownika aktualizacje baz sygnatur, a także historię wykrytych zagrożeń. Ponadto aplikacja ma małe zapotrzebowanie na zasoby systemowe i umożliwia tworzenie list wykluczeń, pozwalających definiować pliki, lokalizacje, rozszerzenia i procesy pomijane podczas skanowania.

Jeśli chodzi o **oprogramowanie przeznaczone do użytku komercyjnego**, a niewątpliwie szkoły do takich użytkowników należą, to sprawa nie jest już taka prosta. Większość oprogramowania antywirusowego tego rodzaju jest płatna. Wersje dla szkół (lub innych instytucji edukacyjnych) są tańsze niż te przeznaczonych dla typowych firm komercyjnych. Często producenci oprogramowania antywirusowego przedstawiają szkołom specjalne oferty i sprzedają swoje produkty po bardzo niskich cenach. Do tego rodzaju oprogramowania należą:

Arcavir 2010 bezpieczna szkoła z ArcaVir RescueDrive (http://www.arcabit.pl) to program antywirusowy polskiego producenta, przeznaczony dla wszystkich komputerów w szkole, posiadający monitor systemu, skaner poczty, *firewall*, skaner stron WWW oraz Bezpieczeństwo rodzinne, dostarczany wraz z pamięcią pendrive, umożliwiającą uruchomienie systemu operacyjnego bezpośrednio z pamięci przenośnej oraz przeskanowanie komputera.

Kaspersky Workspace Security (http://www.kaspersky.pl) to pakiet przeznaczony dla szkół mających do 100 stacji roboczych (za licencję pakietu przeznaczonego do ochrony serwerów plików trzeba dodatkowo zapłacić). Chroni stacje robocze i serwery plików przed wszelkimi rodzajami zagrożeń internetowych, łącznie z wirusami, oprogramowaniem *spyware*, atakami *hackerów* oraz spamem.

MKS_VIR 9.0 Bezpieczna Szkoła (http://www.mks.com.pl) to program antywirusowy przeznaczony dla szkół posiadających do 100 komputerów. Zapewnia pełną ochronę komputera (monitor systemu, skaner dyskowo-plikowy, zaporę sieciową – *firewall*, skaner poczty, filtr spamu oraz monitor rejestru), a także darmową profesjonalną pomoc techniczną w języku polskim. Oprogramowanie dostarczane jest w wersji elektronicznej.

F-secure bezpieczna szkoła (http://www.szkolabezpiecznegointernetu.pl/f-secure) to wielokrotnie nagradzane rozwiązanie zabezpieczające, które zapewnia bezpieczeństwo komputerów podłączonych do Internetu oraz ich pełną wydajność. Dzięki innowacyjnej technologii DeepGuard 2.0., każdy komputer zyskuje kompletną ochronę już w 60 sekund po pojawieniu się nowego zagrożenia. Oprogramowanie ma polską wersję językową, pełne wsparcie techniczne oraz infolinię. Przeznaczony jest dla szkół posiadających do 40 komputerów.

Panda Security Bezpieczn@Szkoła (http://www.pspolska.pl/produkty/oferta_specjalna) – program „Bezpieczn@Szkoła z Panda Security" rozpoczął się 1 października 2008 roku i skierowany jest do dyrektorów szkół publicznych, którzy poszukują kompleksowej ochrony stacji roboczych, serwerów plików i serwerów MS Exchange z centralną konsolą administracyjną. W ramach programu szkoły mogą zakupić w specjalnej cenie roczną licencję bez limitu stanowisk.

Szkoły mogą także skorzystać z darmowego oprogramowania do użytku komercyjnego. W tej grupie programów warto zwrócić uwagę na:

Clam Antywirus (http://clamwin.com) to całkowicie darmowy program antywirusowy, przeznaczony zarówno do użytku osobistego, jak i dla firm. Jego największą wadą jest brak modułu ochrony w czasie rzeczywistym.

Comodo Internet Security (http://www.comodo.com) to pakiet zawierający program antywirusowy i zaporę sieciową, posiadający ochronę w czasie rzeczywistym, całkowicie darmowy, zarówno do użytku domowego, jak i dla firm.

Pisząc o zabezpieczeniu komputerów, nie można pominąć bardzo ważnego oprogramowania, jakim jest zapora sieciowa – tzw. *firewall*. Programy tego typu blokują niepowołany dostęp do komputera poprzez sieć, a także chronią przed wypływaniem danych z komputera do Internetu. W systemach Windows XP wraz z pojawieniem się poprawki ServicePack 2, zapora sieciowa została dodana do systemu, gdzie blokuje nieuprawnione połączenia przychodzące. W systemach Vista oraz Windows 7 zapora potrafi już kontrolować także połączenia wychodzące z komputera. Należy pamiętać, że systemy operacyjne wcześniejsze niż Windows XP SP2 nie posiadają wbudowanej zapory, więc nie należy takich systemów podłączać do Internetu bez zewnętrznej zapory sieciowej.

Na rynku oprogramowania istnieje wiele zapór sieciowych. Są one także wbudowane w pakiety zabezpieczające wraz z antywirusem, tzw. Internet Security. Przykładowo zaporę sieciową posiadają programy Avast czy Comodo Internet Security.

Do popularnych zapór sieciowych, przeznaczonych do użytku domowego, należą:

- Ashampoo FireWall (http://www.ashampoo. com)
- Outpost Firewall Free (http://www.agnitum.com)
- Sunbelt Personal Firewall (http://www.sunbeltsoftware.com)
- Sygate Personal Firewall (http://www.sygate.com)
- ZoneAlarm (http://www.zonelabs.com)

Przy braku zainstalowanego oprogramowania antywirusowego warto skorzystać z możliwości sprawdzenia komputera pod kątem złośliwego oprogramowania przez skaner *online*. Jest to moduł programu antywirusowego, za pomocą którego komputer sprawdza określony przez użytkownika plik lub obszar na dysku twardym, dyskietce czy płycie. Po zakończeniu pracy skaner informuje o liczbie znalezionych wirusów i o tym, ile z nich udało mu się skutecznie usunąć. Aby zastosować skaner, trzeba posłużyć się przeglądarką.

Popularne skanery umożliwiające sprawdzenie komputera znajdują się na stronach:

- http://housecall.trendmicro.com
- http://www.bitdefender.com/scanner/online/free.html
- http://www.pandasecurity.com/homeusers/solutions/activescan
- http://cainternetsecurity.net/entscanner
- http://mks.com.pl/skaner
- http://www.bitdefender.com/scanner/online/free.html
- http://www.arcabit.pl/skaner_on_line

Powyższe skanery potrafią wykryć wirusy, należy pamiętać jednak, że złośliwe oprogramowanie uruchamia się wraz z systemem, dlatego bardzo często skanery online nie są w stanie go usunąć. W takim wypadku pomocne mogą okazać się płyty typu Rescue CD, czyli bootowalne płyty CD (umożliwiające uruchomienie systemu operacyjnego z płyty), zawierające oprogramowanie antywirusowe. Bazują one na różnych dystrybucjach Linuksa i występują w postaci obrazów ISO, które należy wypalić na płycie CD programem do nagrywania płyt (np. darmowy Active@ ISO Burner – http://www.ntfs.com/iso_burner_free.htm).

Należą do nich:

- G-Data Boot CD (http://www.gdata.pl/portal/PL/content/view/116/145)
- Dr. Web LiveCD (ftp://ftp.drweb.com/pub/drweb/livecd)
- ArcaNix (http://bugtraq.arcabit.com/arcanix)
- BitDefender Rescue CD (http://download.bitdefender.com/rescue_cd)
- F-Secure Rescue CD (http://www.f-secure.com/linux-weblog/2009/09/22/rescue-cd-311)
- Vba32 Rescue CD (ftp://anti-virus.by/pub/vbarescue.iso)
- Avira AntiVir Rescue System (http://www.avira.com/en/support/support_downloads.html)
- AVG Rescue CD (http://www.avg.com/us-en/download-file-cd-arl-iso)

Poza wirusami, w Internecie istnieją także programy szpiegujące, tzw. *spyware*, których zadaniem jest gromadzenie informacji o użytkowniku komputera oraz korzystanie z nich bez jego wiedzy. Pomimo że spyware należy do złośliwego oprogramowania, umieszczony został w tym miejscu z dwóch powodów. Po pierwsze, nie wszystkie programy szpiegujące ze względu na swoją „mniej szkodliwą" działalność są wykrywane przez programy antywirusowe, np. potrafią śledzić odwiedzane przez użytkownika strony internetowe i na podstawie ich historii wyświetlać odpowiednie reklamy. Po drugie istnieje specjalistyczne oprogramowanie przeznaczone do wykrywania i usuwania tego typu programów. Do takich aplikacji należą:

- Ad-aware (http://www.lavasoft.com) – program przeznaczony do użytku domowego
- IOBit Security (http://www.iobit.com) – przeznaczony do użytku domowego
- Spybot Search & Destroy (http://www.safer- networking.org) – darmowy, także do użytku komercyjnego

- SUPERAntiSpyware Free Edition (http://www.superantispyware.com) – przeznaczony do użytku domowego
- SpywareBlaster (http://www.javacoolsoftware.com) – przeznaczony do użytku domowego
- Windows Defender (http://www.microsoft.com/poland) – także do użytku komercyjnego, dostępny do pobrania ze strony producenta, jak również poprzez usługę Microsoft Update

Pomimo że powyższe oprogramowanie przeznaczone jest do usuwania oprogramowania typu spyware, potrafi ono także usuwać programy typu Adware czy dialery.

W celu zachowania bezpieczeństwa komputera bardzo istotne i ważne jest systematyczne aktualizowanie systemu operacyjnego i oprogramowania. Działanie takie ma na celu ochronę użytkownika przed oprogramowaniem typu exploit. Ataki ze strony tych programów skierowane są najczęściej na przeglądarki internetowe, jednak zdarzają się także exploity znajdujące się w plikach PDF czy nawet doc. Dlatego, aby uchronić komputer przed tego typu zagrożeniami, należy zawsze na bieżąco aktualizować system i oprogramowanie. Można do tego użyć gotowych programów, których zadaniem jest sprawdzenie aktualnego oprogramowania oraz wyświetlenie dostępnych aktualizacji. Należą do nich:

- Appupdater (http://www.nabber.org/projects/appupdater)
- UpdateStar (http://updatestar.updatestar.com)
- Update Notifier (http://cleansofts.org)

Dbając o bezpieczeństwo komputera, należy zwrócić uwagę także na ochronę prywatności w Internecie. Wszelkie działania (odwiedzane strony, pobrane pliki, zapisane hasła do witryn) wykonywane przy pomocy przeglądarek internetowych umożliwiają ich odtworzenie przez osobę trzecią. Oczywiście każda z przeglądarek internetowych posiada wbudowane mechanizmy do usuwania tych informacji, jednakże warto skorzystać z wyspecjalizowanych pod tym kątem bezpłatnych aplikacji, do których można zaliczyć:

- ATF Cleaner (http://www.atribune.org)
- CCleaner (http://www.piriform.com)
- MRU-Blaster (http://www.javacoolsoftware.com)

Na zakończenie warto dodać, że nie są to wszystkie zagrożenia, z którymi możemy się spotkać w Internecie. Należy zawsze pamiętać, że posiadanie antywirusa, firewalla czy innych programów zabezpieczających nie zapewni 100% bezpieczeństwa, dlatego najważniejsze podczas korzystania z Internetu są profilaktyka i zdrowy rozsądek.

Autor jest starszym specjalistą Działu Technicznego w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

Seks

W grze pojawiają się nagość i/lub zachowania seksualne lub nawiązania do zachowań o charakterze seksualnym.

Hazard

Gry, które zachęcają do uprawiania hazardu lub go uczą.