Zabezpieczenie domowego PC z Microsoft Windows przy korzystaniu z Internetu.

Przemysław Jaroszewski

CERT Polska

Krótki wstęp

Artykuł niniejszy skierowany jest do domowych użytkowników komputerów z systemem Microsoft Windows, którzy łączą się z Internetem, a przede wszystkim tych, którzy korzystają z łącza stałego. Wielu z nich, mimo, że zdaje sobie sprawę z zagrożeń płynących z korzystania z ogólnodostępnej sieci, przy stałym adresie i przez dłuższy czas, rezygnuje z zabezpieczenia swojego komputera, obawiając się, że jest do zbyt trudne dla laika. Mam nadzieję, że wskazówki zawarte w tym materiale pozwolą czytelnikowi na zmianę zdania w tej kwestii.

Aktualizacja systemu

W przypadku każdego systemu operacyjnego podstawową zasadą jego bezpiecznej eksploatacji jest stałe aktualizowanie systemu operacyjnego i posiadanego oprogramowania. W miarę upływu czasu w rozmaitych elementach systemu ujawniane są mniej lub bardziej krytyczne, ze względu na bezpieczeństwo, luki. Producenci reagują na to, publikując odpowiednie łaty i uaktualnienia eliminujące zagrożenie.

W przypadku systemu Microsoft Windows najprostszą metodą utrzymywania systemu w wersji aktualnej jest częste odwiedzanie witryny windowsupdate.microsoft.com. Można również zapisać się na odpowiednią listę dystrybucyjną i otrzymywać informacje wprost do skrzynki pocztowej.

Należy bezwzględnie zainstalować ostatnią wersję Service Pack dla używanego systemu, a następnie wszystkie ważne aktualizacje. Należy także pobrać wszelkie uaktualnienia przeglądarki Microsoft Internet Explorer, z której usług korzysta przy przetwarzaniu kodu HTML wiele aplikacji, a w której wielokrotnie wykrywane i wykorzystywane były bardzo poważne błędy. Warto pamiętać, że jedynym wiarygodnym źródłem uaktualnień Microsoft Windows są strony microsoft.com, a fałszowanie biuletynów i łatek Microsoft jest aktywnie wykorzystywaną metodą

rozpowszechniania tzw. koni trojańskich. Oznacza to, że nie należy ufać listom z informacjami o nowej luce z załączonym programem rzekomo ją eliminującym, a każdą taką wiadomość zweryfikować na stronach Microsoft. Warto również pamiętać, że Microsoft załącza do swoich informacji podpis cyfrowy, na podstawie którego można zweryfikować wiarygodność otrzymanej informacji. Jeśli potrafisz to zrobić to warto pamiętać o tej opcji i sprawdzać oryginalność otrzymanej informacji.

Oprogramowanie antywirusowe

Kolejnym istotnym elementem broniącym domowego komputera powinno być oprogramowanie antywirusowe. Ceny tego oprogramowania są zazwyczaj stosunkowo niskie, a nierzadko bywa ono rozprowadzane bezpłatnie z nowymi komputerami. Stosując takie oprogramowanie nie należy zapominać o regularnej, częstej aktualizacji bibliotek wzorców wirusów. Biorąc pod uwagę obserwowaną prędkość pojawiania się coraz to nowych wirusów, wydaje się, że dla komputera domowego ze stałym łączem cotygodniowa aktualizacja jest absolutnym minimum. Instrukcję aktualizacji wzorców w konkretnym programie powinien dostarczyć jego producent. O ile to tylko możliwe, należy skorzystać z opcji automatycznego uaktualniania bazy programu z zadaną częstotliwością. Oczywiście, najlepszy antywirus nie jest w stanie zapewnić całkowitej szczelności przed złośliwym kodem. Niezbędna jest także świadomość użytkownika, że "nieznane znaczy niebezpieczne". Odwiedzając podejrzane strony, uruchamiając ściągnięte z nich programy lub otwierając załączniki listów, których pochodzenia nie znamy, zawsze ryzykujemy zarażenie bądź uszkodzenie systemu "na własną prośbę".

Domowa zapora ogniowa

Najczęściej zaniedbywanym elementem zabezpieczenia połączenia internetowego, właśnie ze względu na jego skomplikowanie, jest zastosowanie programu filtrującego pakiety czyli tzw. firewalla osobistego (ang. *personal firewall*).

Na rynku istnieje kilka całkiem dobrych pakietów oprogramowania tego typu, dostępnych dla użytkownika domowego całkowicie bezpłatnie. Można wybrać pomiędzy łatwością konfiguracji i czytelnością interfejsu a szczegółowością w filtrowaniu. Zachęcam do zastosowania tego ostatniego typu firewalla osobistego. Kosztem niewielkiego i, co godne podkreślenia, jednorazowego nakładu pracy, można w ten sposób znacząco podnieść poziom zabezpieczenia systemu. Przy wyborze firewall’a należy zwrócić uwagę, aby wybrany program miał możliwość filtrowania pakietów nie tylko ze względu na aplikację, co jest powszechnie

spotykanym rozwiązaniem, ale także na protokół, port oraz adres źródłowy i docelowy. Krótko mówiąc, im więcej szczegółowych możliwości daje nam producent, tym lepiej.

Cenne wskazówki i przykłady bezpiecznej konfiguracji firewalla osobistego można znaleźć na stronie www.tpffaq.com. Co prawda, została ona stworzona z myślą o użytkownikach programu Kerio Personal Firewall i jego właśnie dotyczą szczegółowe opisy reguł tam zawarte, jednak same zasady pozostają niezmienne i mogą być użyte w przypadku innych firewall'i a samo ich zastosowanie nie powinno nastręczyć problemu.

Poniżej znajduje się kilka podstawowych reguł filtrowania, które warto zastosować w konfiguracji swojego firewall'a.

Prawidłowo skonfigurowany firewall osobisty nie powinien:

- zezwalać na udostępnianie plików i drukarek komputerom poza siecią lokalną (jeżeli nie mamy takowej, najlepiej po prostu wyłączyć taką możliwość w konfiguracji właściwości połączenia - zobacz Pomoc na temat udostępniania plików i drukarek),
- zezwalać na odpytywanie o obecność komputera poleceniem *ping*,

Powinien zaś:

- odmawiać wszelkich prób łączenia się z zewnątrz z naszym komputerem (jeżeli chcesz swojego komputera używać jako serwera, prawdopodobnie nie są Ci potrzebne wskazówki z tego artykułu - w przeciwnym razie przemyśl jeszcze raz swoją decyzję).

Jednocześnie normalne czynności, do których wykorzystywane jest połączenie z Internetem, powinny pozostać niezakłócone. W razie jakichkolwiek problemów lepiej poprosić o pomoc znajomego "eksperta", niż zupełnie zrezygnować z osobistego firewall'a.

Archiwizacja danych

Ostatnią, luźno związaną z podłączeniem do Internetu, jednak ściśle powiązaną z samym bezpieczeństwem danych w domowym komputerze, kwestią jest archiwizowanie danych czyli tzw. backup.

We wszystkich wersjach systemu Microsoft Windows znajdują się narzędzia, ułatwiające wykonywanie kopii zapasowych. Przy obecnych, niskich cenach zarówno nagrywarek CD jak i samych nośników CD-R, najprostszym rozwiązaniem może być jednak po prostu skopiowanie najcenniejszych danych na płyty CD. Warto pamiętać, że nie ma sensu archiwizowanie całych dysków, ponieważ praktycznie całe oprogramowanie można odtworzyć, korzystając z dysków instalacyjnych.

Na koniec

Truizmem jest stwierdzenie, że nie istnieje absolutnie pewny sposób zabezpieczenia się przed włamaniem do systemu. Warto jednak zastosować kilka podstawowych, opisanych wyżej "chwytów", które wymagają niewielkiego zaangażowania oraz nakładów finansowych znikomych przy wartości samego komputera, a tym bardziej zawartych na nim danych. Te proste metody są wystarczające, aby zniechęcić ogromną większość potencjalnych włamywaczy od zainteresowania się naszym komputerem, czego sobie i Państwu życzę....

Przydatne adresy:

http://www.microsoft.com/poland

Polska strona Microsoft

http://windowsupdate.microsoft.com/

Windows Update, tu znajdziesz wszystkie potrzebne uaktualnienia

http://www.free-av.com/

http://www.mks.com.pl/

http://www.mcaffee.com/

http://www.symantec.com/

Producenci oprogramowania antywirusowego, także informacje o wirusach

http://www.sygate.com/

http://www.kerio.com/

http://www.looknstop.com/

Producenci oprogramowania typu firewall osobisty

http://www.tpffaq.com/

FAQ na temat osobistych firewalli, w szczególności Kerio Personal Firewall.

http://www.cert.pl/

CERT Polska, aktualne informacje z dziedziny bezpieczeństwa IT