Zaraz po podłączeniu komputera do Internetu zazwyczaj pierwszą technologią, z jaką mamy styczność są strony WWW. Na pulpitach wszystkich komputerów, działających pod kontrolą systemu Windows znajduje się zachęcająca, niebieska ikonka **Internet Explorer**, otwierająca bramę do świata Internetu. Wystarczy kliknąć, wpisać adres i rozpocząć podróż. Powoli...

- **Ale co mi grozi? To tylko tekst i rysunki!**

Pytanie jakie się nasuwa, to dlaczego właściwie strony WWW mogą być groźne dla użytkownika? Wydaje się, że to tylko tekst i rysunki, czasem animacje, które przecież nie mogą nikomu zrobić nic złego. Otóż nie do końca. Wokół stron WWW, przez ostatnie 15 lat ich ewolucji wyrosło wiele technologii, które znacznie wykraczają poza zwykłą prezentację tekstu i grafiki, zbliżając często sposób działania stron do programów znanych z Windows.
Każde rozszerzenie funkcjonalności danej technologii powoduje jej dodatkowe skomplikowanie a co za tym idzie powstają nowe możliwości omijania istniejących zabezpieczeń. Nie należy jednak bać się na zapas. Zmieniając przeglądarkę na inną niż Internet Explorer oraz **aktualizując oprogramowanie** od strony technicznej będziemy względnie zabezpieczeni. Nie są to mury nie do przeskoczenia, ale podobnie jak w przypadku samochodów – im więcej utrudnień na drodze złodzieja tym mniejsza szansa jego powodzenia czy nawet podjęcia jakichkolwiek działań. Po co atakować dobrze zabezpieczony komputer skoro są miliony innych, niezabezpieczonych w ogóle?
Istnieje natomiast znacznie większe zagrożenie, znane pod nazwą **Social Engineering** (Inżynieria społeczna). Jest to w skrócie manipulowanie ludźmi (czyt. najsłabszym ogniwem każdego systemu zabezpieczeń) aby ominąć istniejące, technologiczne zabezpieczenia. Takimi zagrożeniami będziemy się przede wszystkim zajmować w dalszej części artykułu.

- **Patrz gdzie klikasz!**

Wobec tak dużego, jak obecnie, nacisku na bezpieczeństwo programów obsługujących połączenia z Internetem znacznie łatwiej jest osobom o wrogich zamiarach wymusić pewne działania na internaucie, doprowadzając do zainfekowania jego komputera i omijając istniejące zabezpieczenia. Aby się uchronić, należy przede wszystkim kierować się zasadą za zawartą w nagłówku tej części artykułu – **patrz gdzie klikasz!**, albo nieco szerzej: zanim wybierzesz jakąkolwiek funkcję czy odnośnik, upewnij się co do jej celu i przeznaczenia.
Przeglądarki obecnie bardzo często informują użytkownika o potencjalnych zagrożeniach, stąd pierwszym bezpiecznym nawykiem jest **czytać komunikaty przeglądarek** a dopiero później wybierać przyciski, szczególnie "*OK*" lub "*Tak*".
Bardzo często (także na dużych, poważanych stronach WWW) napotkać można bannery (reklamy), które do złudzenia przypominają komunikaty systemu Windows, często informujące o potencjalnym niebezpieczeństwie grożącym systemowi, możliwościach przyspieszenia działania komputera, postępie ściągania wyjątkowo atrakcyjnego filmu – pomysłów jest wiele. Bezpieczeństwo „surfowania" w sieci interesuje nas w momencie, gdy przytrafi się coś złego. Przemierzamy bezkresne zbiory informacji i multimediów, piszemy listy elektroniczne, rozmawiamy ze znajomymi, aż do czasu, kiedy z komputera nagle znikają ważne dokumenty, staje się on niezwykle wolny lub dostawca Internetu odłączy nas od sieci z powodu ogromnych ilości poczty wysyłanej z naszego komputera. Co się dzieje? **Wirus**.

Piszę **wirus**, ponieważ jest to określenie najczęściej padające z ust użytkowników niewtajemniczonych w techniczne aspekty działania Internetu. W rzeczywistości zagrożenia są bardziej zróżnicowane i będziemy się im przyglądać kolejno w dalszej części tej serii.

Wtyczka do gniazdka i…

Tak naprawdę nie potrzeba wiele, aby narazić komputer na niebezpieczeństwo. Wystarczy podłączyć go do sieci, nawet lokalnej. System operacyjny Windows, na którym będziemy się opierali, w ramach starań twórców o jak największą prostotę jego użytkowania nabrał pewnych cech, które ułatwiają ataki na komputer, zarówno przez ludzi jak i zautomatyzowane programy. W kolejnych aktualizacjach stan ten na

szczęście wyraźnie się poprawił i obecnie znacznie większą wagę przykłada się do odpowiednich zabezpieczeń.

I właśnie w zdaniu powyżej znajduje się pierwsze słowo-klucz do bezpieczeństwa – **aktualizacje**. System operacyjny, taki jak Windows to bardzo duże i skomplikowane połączenie wielu programów komputerowych, pisane przez równie duże zespoły ludzi. W takich sytuacjach błędy naruszające bezpieczeństwo są nieuniknione, a że nowe wersje systemu pojawiają się co kilka lat, to pomiędzy nimi wydawany jest szereg aktualizacji, poprawiających rozmaite „dziury".

W ramach zabezpieczenia Windows, Microsoft dodał do niego mechanizm automatycznych aktualizacji, który w momencie wydania nowych „łatek" pobiera je z Internetu i instaluje przy braku ingerencji ze strony użytkownika.

Na samym początku jednak, jeśli kupimy nowy komputer lub zainstalujemy od nowa system, warto ręcznie zadbać o instalację aktualizacji, co można zrobić wchodząc na stronę **Windows Update**. Tam trzeba już tylko postępować według instrukcji, strona sprawdzi, które aktualizacje są już zainstalowane, zaproponuje brakujące, zatwierdzamy domyślne wartości i czekamy na ich ściągnięcie i zainstalowanie, zakończone najczęściej restartem komputera.

Dalsze aktualizacje możemy pozostawić mechanizmowi automatycznemu, warto jedynie upewnić się, iż jest on włączony, wybierając kolejno: *Start* > *Panel Sterowania* > *System* i w otwartym oknie, na zakładce **Automatyczne Aktualizacje** wybrana powinna być pierwsza opcja.

- **Stawiamy mury**

Wszystkim z pewnością obiły się o uszy dwa terminy związane z bezpieczeństwem: **program antywirusowy** oraz **firewall**. Wszyscy to znają, wszyscy powinni mieć, a w rzeczywistości… „przecież nam się na pewno nic złego nie przytrafi". Aż się przytrafi.

Codziennie pojawia się w Internecie od kilku do kilkunastu nowych wirusów, których listę i zagrożenie związane z przyrostem można oglądnąć na stronach firmy Symantec, zajmującej się tworzeniem oprogramowania zabezpieczającego. Aby odpowiednio zabezpieczyć nasz komputer będziemy potrzebowali zarówno firewalla jak i programu antywirusowego.

Ten pierwszy jest już wbudowany w Windows XP i wraz z kolejnymi aktualizacjami jego funkcjonalność została rozszerzona do poziomu, na którym stanowi dosyć dobre zabezpieczenie. Tylko „dosyć", ponieważ mimo wszystko Microsoft nie posiada dużego doświadczenia w tworzeniu tego typu programów a i dotychczasowa forma **Zapory**, jak został on nazwany, pozostawia wiele do życzenia.

Mimo wszystko na początek jest to lepsze niż nic i warto upewnić się, czy dla naszego połączenia z Internetem zapora została włączona. Do tego z Panelu Sterowania wybieramy **Połączenia Sieciowe** i znajdujemy działające połączenie z Internetem (często jedyne). Przy jego ikonie powinna być widoczna niewielka, złota kłódka, oznaczająca funkcjonowanie zapory.

Jeśli kłódki brak, klikamy ikonę połączenia prawym przyciskiem, wybieramy **Właściwości**, zakładkę Zaawansowane i w części oznaczonej **Zapora systemu Windows** klikamy przycisk Ustawienia, po czym w otwartym oknie zaznaczamy opcję włączenia zapory.

Użytkownicy systemów starszych będą musieli, a użytkownicy Windows XP powinni zainteresować się jednak innymi firewallami, które bardzo często w wersjach do użytku domowego są darmowe. Najbardziej znanym jest tutaj **ZoneAlarm**, który można ściągnąć, zainstalować i który w każdej chwili służy użytkownikowi rozległą pomocą.

Samo posiadanie firewalla to jeszcze nie wszystko. W trakcie pracy będzie on potrzebował od użytkownika pewnych **świadomych** decyzji, które programy mogą korzystać z Internetu a które nie. Najczęściej po instalacji nowego programu i po jego uruchomieniu firewall spyta się, czy zezwolić mu na połączenie. Jeśli sami instalowaliśmy ten program to oczywiście należy odpowiedzieć **tak** (i najczęściej zaznaczyć, żeby firewall zawsze się zgadzał), ale wcześniej należy upewnić się, że chodzi właśnie o nasz program – będzie tam podana jego nazwa i kilka dodatkowych informacji. Jeśli nie znamy nazwy, bezpieczniej będzie odpowiedzieć **nie**, po czym sprawdzić dysk programem antywirusowym. Windows nie posiada jednak wbudowanego programu antywirusowego. Być może w niedalekiej przyszłości się to zmieni, o ile sprawdzą się pogłoski o przygotowaniach do wprowadzenia takiego rozwiązania przez Microsoft. Póki co jednak musimy skorzystać z programów innych firm.

Najlepsze rozwiązania są niestety komercyjne i wśród nich na pierwszym miejscu znajduje się [**NOD32**] firmy Eset, który w kolejnych testach magazynu Virus Bulletin wykrywał 100% wirusów, a dodatkowo jest szybki i nie spowalnia w żaden sposób działania komputera.

Z programów darmowych dobrym rozwiązaniem będzie **Avast!** w wersji do użytku domowego, który podobnie zresztą jak NOD32 posiada polskie tłumaczenie.

Oba wspomniane programy posiadają skanery rezydentne, tzn. takie, które działają cały czas bez ingerencji użytkownika, kontrolując wszystkie kopiowane i otwierane pliki oraz programy. Tym samym po ich zainstalowaniu możemy *prawie* zapomnieć o wirusach.

Hasła

Z hasłami dostępu spotkamy się na każdym kroku naszego funkcjonowania w Internecie. Gdziekolwiek dostęp do jakichś zasobów jest kontrolowany – poczta elektroniczna, komunikatory, fora itd. – wymagane będzie zalogowanie się przez podanie wcześniej ustalonych nazwy użytkownika i hasła. Jakość tych haseł będzie się więc bezpośrednio przekładać na poziom zabezpieczenia naszych kont.

Problem pojawia się w ich konstrukcji. Dla administratorów systemów komputerowych najlepsze hasło to długi ciąg losowych znaków, np. „7a68798a8dajkshdal3”, którego oczywiście nie sposób zapamiętać a co dopiero zgadnąć. Dla użytkowników natomiast znakomite hasło to krótkie i proste słowo, np. „misiu”, które szybko można zapamiętać i jeszcze szybciej zgadnąć.

Optymalne rozwiązanie leży pośrodku. Hasłami **nie mogą** być imiona czy nazwiska członków rodziny, osób bliskich, zwierząt domowych, daty urodzin, śmierci, rocznic; ogólnie żadne informacje bezpośrednio związane z nami, ponieważ te stosunkowo łatwo zgadnąć. Nie powinny to być w ogóle istniejące słowa, ponieważ w bardzo prosty sposób można je sprawdzić z pomocą odpowiedniego programu.

Jest natomiast kilka strategii konstruowania haseł, które stosunkowo łatwo zapamiętać a jednak pozostaną bezpieczne. Jedna to zaczynając od jakiegoś słowa, np. „republika” zamienić część liter w nim na cyfry lub znaki, powiedzmy: „r3pub11k4” – można przy tym stosować cyfry przypominające litery, jakie zastępują.

Drugi, prawdopodobnie lepszy sposób to wymyślanie haseł, które brzmią jak słowa, dodając do nich kilka cyfr, np. „poluki483”.

Kolejny problem pojawia się natomiast wraz z rosnącą ilością kont, które rejestrujemy w różnych miejscach. Kuszącą możliwością jest wtedy, aby do każdego stosować to samo hasło. Tego również najlepiej jest zupełnie unikać, ale z drugiej strony mało kto potrafi zapamiętać kilkadziesiąt haseł, więc i tutaj trzeba pójść na kompromis.

Rozwiązaniem, jakie sam stosuję to opracowanie kilku haseł. Najważniejsze, jak hasło dostępu do konta bankowego przez Internet, są całkowicie unikatowe. Takich nie będzie wiele. Pozostałych można utworzyć powiedzmy 3, o różnym stopniu skomplikowania i przy rejestracji w nowym serwisie ocenić jego wagę oraz zastosować odpowiednie hasło. Powiedzmy, że mamy hasła:

- koga729ruty23wero
- zatury43gedna
- sagudo905

Dla głównego konta pocztowego i konta w jakimś serwisie aukcyjnym użyłbym pierwszego, dla blogu i for internetowych drugiego, a dla wszystkich pozostałych stron, które odwiedzam rzadko trzeciego.

Aby dodatkowo ułatwić sobie życie z hasłami, można skorzystać z programu **Password Safe**, który jest… bazą danych haseł, zaszyfrowaną i zabezpieczoną hasłem. Przydaje się szczególnie, kiedy w różnych miejscach mamy różne nazwy użytkownika, jest mały i nie wymaga instalacji, przez co można go nosić nawet ze sobą na pendrive.

W następnej części przeczytacie miedzy innymi o sieciach lokalnych, bezpiecznym korzystaniu z komunikatorów i komputerów publicznych.