Jak bezpiecznie korzystać z komputerów do połączeń z bankowymi systemami transakcyjnymi
(bankowości internetowa, biuro maklerskie, platformy walutowe itp.)

Pomimo zagrożeń, korzystanie z bankowości przez Internet może być bezpieczne. Warunkiem jest odpowiednie zabezpieczenie komputera używanego do połączeń z bankiem oraz stosowanie podstawowych zasad bezpieczeństwa.

Na początek zajmijmy się zagrożeniami - trzeba im się uważnie przyjrzeć, bo tylko kiedy są nam znane, możemy skutecznie się przed nimi bronić. Potem powiemy właśnie o tym, jak to najlepiej robić.

Nierówna walka z *malware*

Liczba wirusów rośnie w zastraszającym tempie – na chwile obecną przyrost liczby nowych wirusów, robaków, Trojanów, szpiegów, *rootkitów* itp. przybrał postać ekspotencjalną (wykładniczą). Producenci oprogramowania antywirusowego nie nadążają z dostarczaniem na bieżąco szczepionek przeciwko lawinowo pojawiającym się i propagowanym w Internecie wirusom. Dodatkowym problemem jest dramatyczny przyrost wielkości baz sygnatur oprogramowania antywirusowego, a im większa jest baza sygnatur, tym bardziej obciążająca komputer jest operacja kontroli antywirusowej. Gdyby oprogramowanie antywirusowe miało pełną bazę sygnatur do wykrywania wirusów, to jego działanie skonsumowałoby w pełni moc procesora komputera. Słowem – komputer zajmowałby się swoim bezpieczeństwem i nic innego w tym czasie nie byłby już w stanie wykonać. Dramatyzmu sytuacji przydaje fakt, iż wirusy pojawiają się w sieci w wielu odmianach – jak wirus grypy. Mówimy tutaj, przez analogię do nauk medycznych, o mutacjach i wielopostaciowości (polimorfizmie) wirusów. Jest rzeczą oczywistą, że im więcej jest takich polimorficznych mutacji, tym bardziej „bezkarny" jest wirus igrający z bezsilnością nawet najlepszych skanerów antywirusowych. Z oficjalnych statystyk wynika, że nawet najlepsze skanery antywirusowe mają bardzo ograniczoną do około 25 procent skuteczność wykrywania i niszczenia wszystkich znanych, obecnych w sieci wirusów. Ta liczba niech mówi sama za siebie.

Co nam grozi?

Dostęp agresorów do naszych danych, zarówno statycznych (te, które są zapisane na dysku twardym komputera lub innych nośnikach danych) jaki i dynamicznych (dane transmitowane przez sieć), jest potencjalnie możliwy na skutek braku elementarnych zabezpieczeń, takich jak:

- Brak oprogramowania antywirusowego lub brak regularnych aktualizacji tegoż;
- Brak regularnych skanów antywirusowych całego komputera;
- Brak zapory sieciowej (firewall) – czy to sprzętowej, w dzisiejszych czasach często spotykanej w routerach klasy Home Office, czy to programowej, instalowanej bezpośrednio na naszym komputerze;
- Stare, nieaktualne i pełne błędów oraz wynikających z nich luk w bezpieczeństwie przeglądarki internetowe
- Brak aktualizacji oprogramowania systemowego (łatki, poprawki, aktualizacje), a także narzędziowego np. stare wersje Acrobat Reader, Java, Flash Player itp.

Z reguły atak na słabo zabezpieczony lub wręcz całkowicie niezabezpieczony komputer polega na wykorzystaniu przez agresora podatności, czyli luki w bezpieczeństwie, określonej – będącej celem ataku - aplikacji. Taka luka jest najczęściej skutkiem błędów na poziomie kodu czy konfiguracji oprogramowania. Agresor wykorzystuje coś w rodzaju dopasowanego do luki wytrycha (ang. *exploit*), mającego przeważnie postać niewielkiego kodu wykonywalnego, do zaatakowania komputera, na którym działa podatna aplikacja. Skala ataku i jego efekty zależą

jedynie od fantazji agresora – od niewinnego podglądania co robi użytkownik komputera, po całkowite przejęcie nad nim kontroli, co często wiąże się także z wykorzystaniem komputera do przeprowadzenia czynności nielegalnych np. wysyłanie spamu, ataki na inne komputery, pranie pieniędzy itp.

Przyjrzyjmy się etap-po-etapie przypadkowi z życia wziętemu: (1) Eksperci od bezpieczeństwa lub hakerzy wykrywają podatność w kodzie przeglądarki internetowej. Podatność ta ujawnia się, kiedy w oknie przeglądarki internetowej są prezentowane „odpowiednio spreparowane" grafiki. One to właśnie stanowią w tym przypadku kod wytrycha. (2) W ślad za pojawieniem się w Internecie informacji o wystąpieniu podatności, agresor przygotowuje specjalne strony internetowe, na których publikowane są tego typu właśnie grafiki z zamiarem ich prezentowania internautom - potencjalnym ofiarom ataków. Grafiki wyglądają z pozoru niewinnie. W oknie przeglądarki prezentują się normalnie. Jedyna różnica pomiędzy nimi, a normalnymi grafikami polega na tym, że gdzieś w treści pliku grafiki-wytrycha zawarta jest sekwencja kodu wrogich poleceń agresora, do natychmiastowego wykonania na zaatakowanym komputerze. (3) Wspomniany kod jest automatycznie wykonywany z chwilą wyświetlenia grafiki w oknie przeglądarki internetowej. Dzieje się to w sposób na ogół całkowicie niezauważalny dla ofiary ataku. Milczy przeważnie program antywirusowy i inne zabezpieczenia komputera, bo atak jest na tyle „świeży", że producenci oprogramowania zabezpieczającego nie zdążyli jeszcze opracować przeciwko niemu skutecznej szczepionki. W rezultacie udanego ataku, agresor przejmuje zdalną kontrolę nad komputerem ofiary i od teraz może z nim zrobić wszystko, na przykład zainstalować oprogramowanie złośliwe, wykraść pliki z dysku, wyłączyć systemy zabezpieczeń, uruchomić „szpiega" – program śledzący dalsze działania użytkownika na zaatakowanym komputerze, „podsłuchać" i wykraść hasła, numery kart kredytowych czy podmieniać transakcje w bankowości internetowej.

W opisanym przypadku przyczyną ataku było zaniedbanie aktualizacji oprogramowania przeglądarki internetowej. Niestety, typową wobec konieczności takowej aktualizacji jest postawa użytkownika wyrażona w słowach: „kto by tam o tym pamiętał, przecież to tylko przeglądarka czy zwykły *Acrobat Reader*, jaki to może mieć związek z bezpieczeństwem informacji i komputera?" – i lubi się ona mścić. Jeśli połączona jest ze skłonnościami do surfowania po podejrzanych stronach WWW (strony pornograficzne, strony udostępniające kody aktywacyjne do nielegalnie ściągniętego oprogramowania itp.), wówczas efekt może być dramatyczny.

Jak się bronić?

Przechodzimy do sedna sprawy. Najlepszym sposobem ochrony jest stosowanie na co dzień podstawowych zasad bezpieczeństwa: niepobieranie z Internetu niezaufanego oprogramowania, unikanie surfowania po podejrzanych stronach WWW, bieżąca aktualizacja (najlepiej automatyczna aktualizacja) i instalacja „łatek" systemu operacyjnego oraz oprogramowania użytkowego. Ważne jest oczywiście posiadanie dobrego oprogramowania antywirusowego, a najlepiej pakietu zintegrowanych narzędzi do ochrony komputera, zawierającego obok skanera antywirusowego dodatkowo osobistą zaporę sieciową (ang: *Personal Firewall*), osobisty system przeciwdziałania włamaniom (ang: *Host Intrusion Prevention System*) itp. Najskuteczniejsze są te narzędzia, których działanie nie polega wyłącznie na analizie sygnatur lecz opiera się także na blokowaniu behawioralnym. Pod tym skomplikowanym terminem kryje się rzecz prosta – blokowanie niewłaściwych lub podejrzanych operacji uruchomionego na komputerze oprogramowania (na przykład prób kasowania plików systemowych, nadpisywania ważnych dla działania komputera struktur dysku, nawiązywania połączeń do różnych podejrzanych miejsc, wysyłania dużej ilości „śmieciowych" danych, próby zarażania innych komputerów, nieuprawnionego instalowania na komputerze różnych programów, próby logowania na konta użytkowników uprzywilejowanych, rozsyłanie spamu itp.).

Skuteczność narzędzi, to nie wszystko. Trzeba ich jeszcze właściwie używać, co w praktyce sprowadza się do wykonywania częstych skanów antywirusowych, nielekceważenia komunikatów i ostrzeżeń, podejmowania

natychmiastowych działań w odpowiedzi na istotne alerty z systemów ochrony komputera o przełamaniu jego zabezpieczeń itp.

Jak korzystać bezpiecznie z komputera i nie dać się zwariować?

Komputer to nie tylko korzystanie z Internetu, poczty i innych usług online. Komputer wykorzystujemy na co dzień do dostępów do innych systemów, w tym na przykład do systemów transakcyjnych banku, więc naturalną koleją rzeczy, od jego bezpieczeństwa zależy w dużym stopniu bezpieczeństwo naszych danych i finansów.
Dbałość o bezpieczeństwo komputera musi być wręcz – jak dbałość o codzienną higienę - żelaznym elementem naszego stylu życia.

Aby korzystanie z tego typ usług było bezstresowe i bezpieczne dla nas i naszego portfela, należy pamiętać o podstawowych, elementarnych zasadach bezpieczeństwa:

- Nie powinniśmy udostępniać swoich komputerów osobom postronnym. Powinniśmy zadbać o zabezpieczenie swojego sprzętu przed kradzieżą, zagubieniem, uszkodzeniem, zniszczeniem i nieuprawnionym użyciem. W szczególności, powinniśmy zadbać o bezpieczeństwo komputera pozostawianego bez osobistego nadzoru.
  Szczególna dbałość o fizyczne bezpieczeństwo komputerów oznacza między innymi: niepozostawianie urządzeń w samochodzie i w pokojach hotelowych oraz ciągły nadzór nad komputerem w podróży. Podczas podróży publicznymi środkami transportu (autokar, samolot) laptopa należy zawsze przewozić jako bagaż podręczny.

- Hasła powinny być traktowane przez każdego z nas tak, jak traktuje się klucz do skarbca. Wiadomo, że utrata tego klucza oznacza kłopoty i ma przeważnie bardzo poważne konsekwencje. Podobnie jest z hasłami - ujawnienie ich skutkuje zagrożeniem nieuprawnionego dostępu do systemu przez niepowołane osoby ze wszystkimi tego bolesnymi konsekwencjami. Warto więc pamiętać o podstawowych zasadach bezpieczeństwa: (1) tworzenia haseł, (2) posługiwania się nimi oraz (3) zarządzania nimi (zmiana, przechowywanie).

Przy tworzeniu hasła powinniśmy pamiętać o następujących zasadach:

- Hasła nie powinny być frazami słownikowymi (polskimi i obcojęzycznymi);
- Hasło powinno zawierać więcej niż 7 znaków;
- Hasło nie powinno bazować na znanych danych osobowych użytkownika lub być znaną powszechnie nazwą czy identyfikatorem, jak na przykład imieniem (własnym, przyjaciela, członka rodziny itp.), nazwiskiem, nazwą (na przykład systemów, poleceń, programów, procesów itp.), nazwą organizacji lub jej struktur, datą (datą urodzin, datą dobrze znanych wydarzeń historycznych itp.), adresem, numerem telefonu oraz kombinacjami wymienionych fraz;
- Hasło nie może być powtarzalną kombinacją znaków (na przykład aaabbbccc), łatwo przewidywalną sekwencją znaków (na przykład 12345, qwerty itp.) lub ich odwrotną transpozycją (np. 54321);
- Hasło nie może być prostą kombinacją jednej ze wspomnianych fraz wraz z cyfrą na początku lub na końcu (na przykład secret1 czy 1secret);
- Silne hasło musi zawierać kombinację zarówno małych jak i dużych liter oraz znaków specjalnych (na przykład takich jak !@#$%^&*()_+|~-=\`{}[]:";'<>?,./));
- Zalecanym sposobem tworzenia silnych haseł są tzw. pass-frazy, tworzone zgodnie z następującym schematem: (1) należy opracować zdanie bazowe do pass-frazy, na przykład „Czy można stworzyć bezpieczne hasło?", (2) należy wyróżnić w zdaniu bazowym elementy pass frazy, na przykład „Czy można stworzyć bezpieczne hasło?", (3) należy dokonać mapowania i podmiany znaków (zmiana wielkości, znaki

specjalne: Czy → 3; m → M; s → s; b → B; has → # (od hasz), ło? → 1o?), w wyniku czego powstaje silna pass-fraza, na przykład: 3MsBez#1o?

Posługując się hasłami powinniśmy pamiętać o tym, aby:

- nie używać takich samych haseł do uwierzytelnień we wszystkich systemach, do których się logujemy. Na przykład nie powinniśmy stosować do logowania się do banku identycznego hasła, jak hasło do systemów pocztowych czy portali społecznościowych (z portali społecznościowych czy z publicznych systemów pocztowych coraz częściej wyciekają różne informacje, zatem trzeba dbać o to, aby wyciek danych z takich systemów nie oznaczał jednocześnie ujawnienia naszego hasła do bankowości internetowej);
- nie współdzielić hasła z innymi użytkownikami (nawet członkami rodziny);
- nie ujawniać haseł innym osobom (w bezpośredniej rozmowie, przez telefon, w wiadomościach poczty.

Ponieważ pierwszy z powyższych postulatów może być (w przypadku osób korzystających z wielu różnych usług internetowych) trudny i uciążliwy w realizacji, jako absolutne minimum należy przyjąć stosowanie różnych haseł w oddzielnych grupach usług: inne dla kont pocztowych, inne w portalach społecznościowych, a jeszcze inne (i najlepiej istotnie trudniejsze do odgadnięcia oraz szczególnie pieczołowicie chronione) do usług bankowości internetowej.

Podstawowe zasady bezpiecznego zarządzania hasłami to:

- Niezapamiętywanie haseł w systemach i aplikacjach, chyba że zapisujemy hasło w specjalnie do tego celu przeznaczonej aplikacji (tzw. *Password Manager*), przechowującej hasła w szyfrowanych bazach;
- Niezapisywanie haseł w postaci jawnej, możliwej do odczytania przez niepowołane osoby;
- Hasła powinny być regularnie zmieniane, przynajmniej raz na dwa miesiące. Ponadto, hasła muszą być zmienione natychmiast w sytuacji, kiedy zachodzi prawdopodobieństwo ich ujawnienia niepowołanym osobom.

Powinniśmy unikać uruchamiania wykonywalnych plików (na ogół z rozszerzeniami nazw .EXE, .COM, .BAT, .DLL, .CMD, .VBS, .VBE lub .PIF) otrzymanych w załącznikach poczty elektronicznej. To samo odnosi się do pobierania i uruchamiania wykonywalnych plików ze stron WWW oraz kopiowania danych z niesprawdzonych nośników.

Kończąc temat bezpieczeństwa korzystania z komputerów, warto pokusić się o krótką puentę: bezpieczeństwo jest zawsze wypadkową zastosowania tak rozwiązań technicznych, jak i zachowań użytkownika. Zawsze też decyduje tu najsłabszy element. Na nic zda się nam nawet najdoskonalszy system, jeśli będziemy uporczywie lekceważyć wszelkie jego ostrzeżenia o zagrożeniach oraz zaniedbywać podstawowe zasady bezpieczeństwa korzystania z komputera.