Zasady bezpiecznej pracy z dziennikiem elektronicznym „MobiReg”.

Bezpieczne hasło

Wymagane są hasła o **minimalnej długości 8 znaków**. Hasła muszą obowiązkowo zawierać **dużą i małą literę oraz cyfrę lub znak specjalny**. Jak łatwo stworzyć łatwe do zapamiętania a jednocześnie bezpieczne hasło można przeczytać tu. Hasła nie powinny bazować na naszych danych personalnych, napisach dostępnych z miejsca logowania, takich jak np. nr seryjny komputera, symbol czy też nazwa monitora lub drukarki. Hasłem stosunkowo łatwym do odgadnięcie są też sekwencje klawiszy układające się w charakterystyczny sposób na klawiaturze Przykłady niebezpiecznych haseł spełniających formalne wymogi: Robert150860 – imię+data urodzenia, Maserati3200GT – model samochodu, Qwert^&* - sekwencja kolejnych przylegających do siebie klawiszy, Zaq!2wsX – jak poprzednio, Administrator2 – hasło bazuje na loginie, (takie hasło posiadał administrator serwisu Komitetu Rady Ministrów, przed przejęciem go przez hackera), 0kularn1k - bazuje na słowie Okularnik z prostym zastąpieniem litery O – zerem i litery i cyfrą 1. Tego typu proste i intuicyjne zastąpienia są obecnie obsługiwane przez łamacze haseł. Najlepsze hasła to hasła wygenerowane automatycznie. Dobrym obyczajem jest okresowa zmiana hasła. W przypadku mozliwości ujawnienia hasła należy je natychmiast zmienić. Hasła nie wolno nikomu ujawniać, ani administrator szkolny, ani firma Mobireg.pl nigdy nie poprosi Cię o hasło.

Bezpieczny komputer

Komputer wykorzystywany do pracy z dziennikiem elektronicznym musi być wyposażony w legalny, wspierany przez producenta system operacyjny z zainstalowanymi wszystkimi aktualizacjami (np. Windows XP nie jest już wspierany). Ponadto powinien mieć zainstalowane aktualne oprogramowania antywirusowe i antyszpiegowskie wraz z aktualną bazą wirusów i trojanów uniemożliwiające zainstalowanie trojana lub keyloggera. Szczególnie dotyczy to komputerów stacjonarnych stojących w pracowniach. W przypadku pracy wielu nauczycieli na jednym komputerze zalecana jest praca na odrębnych kontach użytkownika. Konta użytkowników powinny być chronione hasłem. Uczniowie nie mogą mieć na komputerze nauczycielskim, na którym pracuje dziennik elektroniczny konta o uprawnieniach administratora. Musimy mieć gwarancję, że komputer nie ma zainstalowanego szkodliwego oprogramowania.

Bezpieczne zachowania:

1. Logujemy się tylko na bezpiecznych komputerach, nie logujemy się na nieznanych komputerach: uczniowskich, dostępnych publicznie lub niespełniających w/w warunków bezpiecznego komputera.
2. Zawsze sprawdzamy, czy połączenie jest połączeniem szyfrowanym, czyli zabezpieczonym przed podsłuchem z uwierzytelnioną certyfikatem domeną. Połączenia takie oznaczone jest kłódką.
3. Po zakończonej sesji wylogowujemy się. Nie wychodzimy z pomieszczenia w trakcie sesji z programem. Nie zostawiamy komputera z otwartą sesją Windows bez nadzoru.
4. Używamy wyłącznie bezpiecznych haseł. Nie ujawniamy haseł nikomu. Ignorujemy mail-e pochodzące proszące o podanie hasła od rzekomych administratorów. Prawdziwy administrator nie potrzebuje znać naszego hasła.
5. Hasło w czasie logowania wpisujemy tak, by dłonie były niewidoczne dla uczniów. Na notebook-u zwykle ekran zasłania nasze dłonie, na komputerze stacjonarnym należy klawiaturę umieścić tak, by zasłaniał ją ekran lub jednostka centralna. W przypadku podejrzenia ujawnienia hasła należy bezwzględnie je zmienić.
6. Jeśli w szkole używane są tablety z systemem android, to nie wolno udostępniać ich uczniom. Podobnie jak na komputerze istnieje na tablecie możliwość zainstalowania oprogramowania szpiegowskiego, wykradającego loginy i hasła.

Słowniczek – słowa, które warto znać

Trojan – (źródło: Wikipedia) określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje dodatkowo implementuje niepożądane, ukryte przed użytkownikiem różne funkcje (programy szpiegujące, bomby logiczne, furtki umożliwiające przejęcie kontroli nad systemem przez nieuprawnione osoby itp.). Nazwa pochodzi od mitologicznego konia trojańskiego.

Programy szpiegujące – (źródło: Wikipedia) (ang. *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 należeć mogą:

- adresy www stron internetowych odwiedzanych przez użytkownika
- dane osobowe
- numery kart płatniczych
- hasła
- zainteresowania użytkownika (np. na podstawie wpisywanych słów w oknie wyszukiwarki)
- adresy poczty elektronicznej
- archiwum

Keylogger – (źródło: Wikipedia) (ang. "key" – klawisz, "log" – dziennik) – rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika komputera. Częściej spotykane są keyloggery programowe Programy te działają na zasadzie przejęcia kontroli nad procedurami systemu operacyjnego służącymi do obsługi klawiatury. Dzięki takim zabiegom mogą przechwytywać komunikaty o wciśniętych klawiszach. Zaawansowane keyloggery mogą posiadać ponadto takie funkcje jak:

- przechwytywanie zrzutów ekranu.
- wysyłanie logów i zrzutów na e-mail lub serwer ftp.
- pobieranie informacji o aktywnych oknach i programach.
- chroniące przed wykryciem poprzez:
    - ukrywanie się na liście programów uruchamianych na starcie systemu.
    - ukrywanie się w menadżerze zadań.
    - ukrywanie i szyfrowanie pliku gdzie zapisywane są logi.
    - szyfrowanie połączenia z serwerem[1].

Inżynieria społeczna, **inżynieria socjalna**, **socjotechnika** – (źródło: Wikipedia) w bezpieczeństwie teleinformatycznym zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę. Hackerzy często wykorzystują niewiedzę bądź łatwowierność użytkowników systemów informatycznych, aby pokonać zabezpieczenia odporne na wszelkie formy ataku. Wyszukują przy tym najsłabszy punkt systemu bezpieczeństwa, którym jest człowiek.

Komputerowi oszuści często podają się za inne osoby, aby wyłudzić od swoich ofiar cenne dane. Cracker może dla przykładu podać się za administratora banku i przesłać ofiarom adres swojej strony, która łudząco przypomina stronę banku internetowego. Dzięki opanowaniu inżynierii socjalnej oszust wie, że przeciętny użytkownik nigdy nie sprawdza, czy strona jego banku jest oznaczona kłódką symbolizującą nawiązanie bezpiecznego połączenia. Nieostrożni klienci pozostawiają internetowemu złodziejowi swoje dane, które ten może wykorzystać do oczyszczenia ich kont z pieniędzy. Działanie opisane w tym przykładzie określane jest nazwą „phishing".