INFORMACJA O SZCZEGÓLNYCH ZAGROŻENIACH ZWIĄZANYCH Z KORZYSTANIEM Z USŁUG ŚWIADCZONYCH DROGĄ ELEKTRONICZNĄ

Administrator sklepu internetowego ARMATURA informuje, że szczególnymi zagrożeniami związanymi z korzystaniem z usługi świadczonej drogą elektroniczną są:

1. możliwość otrzymania spamu, czyli niezamówionej informacji handlowej przekazywanej drogą elektroniczną;
2. obecność i działanie oprogramowania typu malware, w tym wirusów komputerowych, czyli szczególnego oprogramowania, które jest w stanie, po uruchomieniu, zarazić pliki w sposób samopowielający, zazwyczaj nie będąc zauważonym przez użytkownika; wirusy mogą być mniej lub bardziej szkodliwe dla systemu operacyjnego, w którym się znajdują, ale nawet w najmniej poważnym przypadku są marnotrawstwem pamięci RAM, CPU i miejsca na twardym dysku.
3. obecność i działanie robaków internetowych (worm), czyli szkodliwego oprogramowania zdolnego do samopowielania; e-mail worm jest niszczącym atakiem przeciwko sieci, polegającym na zebraniu wszystkich adresów e-mail znajdujących się w lokalnym programie (na przykład w MS Outlook) i wysłaniu na nie setek e-maili zawierających robaka w niewidocznym załączniku;
4. możliwość zadziałania oprogramowania typu spyware, to jest oprogramowania szpiegującego działania użytkownika w Internecie, instalującego się bez jego wiedzy, zgody i kontroli;
5. możliwość bycia narażonym na cracing lub phishing (łowienie haseł) - w kontekście informatycznym phishing oznacza technikę łamania zabezpieczeń (cracking), używaną do pozyskania osobistych i poufnych informacji w celu kradzieży tożsamości, poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne;
6. piractwo - termin używany przez piratów komputerowych do określenia oprogramowania, z którego zdjęto zabezpieczenie przed kopiowaniem i które udostępniono w Internecie, skąd może być pobrane;
7. sniffing - niedozwolony podsłuch, inny niż mieszczący się w granicach pojęcia cracking i phising, polegający na wykorzystaniu sniffera - programu komputerowego, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci;
8. czynności kryptoanalizy, to jest odnalezienia słabości systemu kryptograficznego, a tym samym umożliwienia jego złamania lub obejścia;
9. możliwość bycia narażonym na działania innego niechcianego lub "złośliwego" oprogramowania, wykonującego czynności niezamierzone przez użytkownika, niewchodzące w granice definicji wymienionych powyżej, a występujące pod nazwami: wabbit, trojan, backdoor, exploit, rootkit, keylogger, dialer, hoax.