ZAŁĄCZNIK NR 3

INFORMACJA O SZCZEGÓLNYCH ZAGROŻENIACH ZWIĄZANYCH Z KORZYSTANIEM Z USŁUGI ŚWIADCZONEJ DROGĄ ELEKTRONICZNĄ

Sprzedawca niniejszym informuje Użytkowników Sklepu o szczególnych zagrożeniach bezpieczeństwa jakie się mogą wiązać z korzystaniem z usługi świadczonej drogą elektroniczną. Tego rodzaju zagrożenia mogą pojawiać się np. w przypadku usług łączności elektronicznej świadczonych za pomocą otwartej sieci, takiej jak Internet. Zaradzenie takim zagrożeniem leży poza zakresem możliwości Sklepu. Najczęściej będą to następujące zagrożenia:

- **możliwość otrzymania spamu, czyli niezamówionej informacji reklamowej (handlowej) przekazywanej drogą elektroniczną,**
- **możliwość bycia narażonym na:**
- **obecność i działanie oprogramowania typu malware czyli ogółu programów o szkodliwym działaniu w stosunku do systemu komputerowego lub jego użytkownika,**
- **działanie robaków internetowych (worm), czyli szkodliwego oprogramowania zdolnego do samopowielania,**
- **zadziałanie oprogramowania typu spyware, programu szpiegującego działania użytkownika w Internecie, instalującego się bez jego wiedzy, zgody i kontroli,**
- **cracking – dziedzina łamania zabezpieczeń (najczęściej cracking sieciowy i oprogramowania),**
- **phishing - metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej),**
- **sniffing - program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualnie analizowanie danych przepływających w sieci,**
- **piractwo – w szczególności nieuprawnione kopiowanie i wynajem oprogramowania.**
- **nielegalna ingerencja w system, która powodująca poważne zakłócenia w funkcjonowaniu systemu komputerowego na skutek wprowadzania, (transmisji), uszkodzenia, usunięcia, pogorszenia, zmiany lub zablokowania danych.**
- **Inne.**

Sprzedawca wskazuje jednak na podstawowe metody zabezpieczania systemu, które mogą zwiększyć poziom bezpiecznego korzystania min. z serwisów internetowych:

- **Korzystanie z serwisów tylko na zaufanych urządzeniach (komputer, tablet, telefon etc.) z zainstalowanym legalnym systemem operacyjnym.**
- **Regularna aktualizacja posiadanego systemu operacyjnego oraz innych aplikacji (w szczególności przeglądarki internetowe, wtyczki flash, klientów poczty, przeglądarki pdf itp.). Aktualizacje legalnego oprogramowania często naprawiają luki w bezpieczeństwie, które starają się wykorzystać oszuści.**
- **Używanie zapór (firewall), które pomagają chronić komputer przed atakami z sieci,**
- **Regularne wykonywanie kopii bezpieczeństwa,**
- **Unikanie podejrzanych próśb,**
- **Unikanie podejrzanych e-maili,**
- **Unikanie podejrzanych stron internetowych.**