Załącznik nr 2 do Regulaminu serwisu internetowego https://zabawkismart.pl/

Informacja o szczególnych zagrożeniach związanych z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną

Korzystanie z Internetu, w tym również korzystanie z usług w drodze elektronicznej może wiązać się z różnymi zagrożeniami, w szczególności takimi jak:
1) możliwość otrzymania spamu, czyli niezamówionej informacji reklamowej (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. Malware to termin ogólny, który dotyczy niepożądanego oprogramowania, w tym wirusy, robaki, konie trojańskie, *ransomware, spyware, adware, scareware* i inne szkodliwe programy;
3) obecność i działanie robaków internetowych (worm), czyli szkodliwego oprogramowania zdolnego do samopowielania;
4) możliwość zadziałania oprogramowania typu *spyware*, które szpieguje działania użytkownika w Internecie, instalującego się bez jego wiedzy, zgody i kontroli;
5) możliwość bycia narażonym na *cracking* lub *phishing* (łowienie haseł), które łączą się z możliwością łamania zabezpieczeń przez osoby trzecie i używania ich do pozyskania osobistych i poufnych informacji w celu kradzieży tożsamości, poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne itp.;
6) *sniffing* – niedozwolony podsłuch, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci;
7) *hacking* – działania tak zwanych hackerów, zmierzających do włamania się do systemu usługodawcy (np. ataki na jego stronę internetową), jak i do systemu usługobiorcy;
8) 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* i inne.

Sprzedawca nie ma wpływu na działanie Internetu i na zagrożenia z nim związane. Sprzedawca stale podejmuje działania podnoszące bezpieczeństwo działania jego witryny internetowej, jednak nie ma możliwości całkowitego wyeliminowania ryzyka ingerencji osób trzecich. W związku z powyższym, aby uniknąć zagrożeń, ważne jest, by Klient zainstalował na swoim urządzeniu elektronicznym program antywirusowy i stale go aktualizował, a także aby stale aktualizował zainstalowane na swoim urządzeniu programy komputerowe. Ponadto istotne jest, aby użytkownicy dokonujący za pośrednictwem sieci Internet tzw. "płatności elektronicznych" w sposób szczególny chronili informacje zawierające dane o numerach rachunków bankowych, kart kredytowych, haseł do logowania itp., przed ich ujawnieniem osobom trzecim.