Załącznik nr 1

DO REGULAMINU ŚWIADCZENIA USŁUG DROGĄ ELEKTRONICZNĄ

INFORMACJA O SZCZEGÓLNYCH ZAGROŻENIACH ZWIĄZANYCH Z KORZYSTANIEM PRZEZ KLIENTÓW Z USŁUG ŚWIADCZONYCH DROGĄ ELEKTRONICZNĄ PRZEZ SPRZEDAWCĘ,

Sprzedawca, wykonując obowiązek z art. 6 pkt 1) ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2017 r. poz. 1219), informuje o szczególnych zagrożeniach związanych z korzystaniem przez Klientów z usług świadczonych drogą elektroniczną. Informacja niniejsza dotyczy zagrożeń, które mogą wystąpić jedynie potencjalne, ale które powinny być brane pod uwagę, mimo stosowania przez Sprzedawcę środków zabezpieczających infrastrukturę Sklepu Internetowego przed nieuprawnionym działaniem osób trzecich. Do podstawowych zagrożeń związanych z korzystaniem z sieci Internet należą:

1) złośliwe oprogramowanie (ang. malware) – różnego rodzaju aplikacje lub skrypty mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do systemu teleinformatycznego użytkownika sieci, takie jak wirusy, robaki, trojany (konie trojańskie), keyloggery, dialery;
2) programy szpiegujące (ang. spyware) – programy śledzące działania użytkownika, które gromadzą informacje o użytkowniku i wysyłają je - zazwyczaj bez jego wiedzy i zgody - autorowi programu;
3) spam - niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym;
4) wyłudzanie poufnych informacji osobistych (np. haseł) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. phishing);
5) włamania do systemu teleinformatycznego użytkownika z użyciem m.in. takich narzędzi hackerskich jak exploit i rootkit.

Klient, aby uniknąć powyższych zagrożeń, powinien w sytuacji, gdy korzysta z Internetu, zainstalować na własnych urządzeniach program antywirusowy, który powinien być na bieżąco aktualizowany. Ochronę przed zagrożeniami związanymi z korzystaniem przez Klientów z usług świadczonych drogą elektroniczną zapewniają także, włączona zapora sieciowa (ang. firewall), aktualizacja wszelkiego oprogramowania, wyłączenie makr w plikach MS Office nieznanego pochodzenia, regularne całościowe skany systemu programem antywirusowym i antymalware, instalacja programów prewencyjnych (wykrywania i zapobiegania włamaniom), szyfrowanie transmisji danych, nieotwieranie załączników poczty elektronicznej niewiadomego pochodzenia, czytanie okien instalacyjnych aplikacji, a także ich licencji.