Informacja
o szczególnych zagrożeniach związanych z korzystaniem z usługi świadczonej drogą elektroniczną

Stosownie do treści art. 6 pkt 1 ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002.144.1204 z późniejszymi zmianami) Katarzyna Podyma prowadząca Kancelarię Radcy Prawnego Katarzyna Podyma, ze stałym miejscem wykonywania działalności gospodarczej w Katowicach (40-078), pl. Wolności, nr 3, lok. 3A, NIP: 6291667024 (zwana dalej **Usługodawcą**) informuje niniejszym o następujących potencjalnych zagrożeniach związanych z korzystaniem z usług świadczonych drogą elektroniczną:

1. ingerencja osób trzecich w bazy danych dotyczących Użytkownika, w tym przeglądanie, kopiowanie, modyfikacja i kasowanie danych dotyczących Użytkownika,
2. ingerencja osób trzecich w transmisję informacji pomiędzy systemem teleinformatycznym Użytkownika a systemem teleinformatycznym Usługodawcy,
3. otrzymanie niezamówionej informacji handlowej (spam) w drodze elektronicznej,
4. zainfekowanie systemu teleinformatycznego oprogramowaniem typu malware (złośliwe oprogramowanie, w tym wirusy i robaki komputerowe, konie trojańskie), spyware (programy szpiegujące),
5. wyłudzanie poufnych informacji (phishing) oraz łamanie zabezpieczeń oprogramowania (cracking),
6. przełamanie protokołów kryptograficznych wykorzystywanych w wymianie informacji pomiędzy systemami teleinformatycznymi, a w konsekwencji umożliwienie w szczególności podsłuchiwanie przekazywanych informacji,
7. podrabianie protokołów i certyfikatów bezpieczeństwa zabezpieczających strony internetowe,
8. instalacja i korzystanie z oprogramowania niezbędnego do korzystania z usługi zapewnianej przez Usługodawcę z nieoficjalnych i nieautoryzowanych źródeł czy instalacja i korzystanie z oprogramowania pirackiego – oprogramowanie takie zawierać może szkodliwe oprogramowanie wskazane powyżej, może posiadać obniżony poziom zabezpieczeń z uwagi na brak aktualizacji mających na celu zwiększenie ochrony oprogramowania przed nieuprawnionym dostępem,

Wskazane powyżej przypadki nieuprawnionej ingerencji osób trzecich lub ich bezprawnych działań, skutkować mogą uzyskaniem przez osoby nieupoważnione dostępu do sieci telekomunikacyjnej Usługodawcy jak i Użytkownika, w tym poszczególnych komputerów wchodzących w skład tej sieci, a także zakłóceniem lub całkowitym wyłączeniem funkcjonowania urządzeń, w tym oprogramowania wchodzącego w skład sieci lub przejęcia nad nim kontroli. Działania te skutkować mogą uzyskaniem przez osoby trzecie informacji gromadzonej w systemie teleinformatycznym, w szczególności w bazach danych a także informacji niezbędnych dla dokonania płatności elektronicznych.

Usługodawca podejmuje niezbędne działania mające na celu minimalizację ryzyka wystąpienia zagrożeń wskazanych powyżej a także podnoszące bezpieczeństwo komunikacji z Serwisem. Niezależnie od tego, Usługodawca zaleca zaopatrzenie komputera Użytkownika w aktualne oprogramowanie typu antywirus oraz firewall a także ich bieżące aktualizowanie, jak również wdrożenie wewnętrznych procedur, mających na celu ochronę loginów i haseł zapewniających dostęp do systemu teleinformatycznego oraz usług świadczonych w drodze elektronicznej, przed dostępem osób nieupoważnionych. Zaleca się, aby hasła i loginy przyznane Użytkownikowi, nie były udostępniane innym osobom, nawet za zgodą Użytkownika.

Usługodawca informuje ponadto, że podejmowane środki ochrony (w tym antywirusowej, firewall), nie zapewniają pełnej ochrony przed możliwą ingerencją osób trzecich w system teleinformatyczny, nie mniej ich stosowanie może ograniczyć ryzyko wystąpienia niepożądanych działań.

Usługodawca zaleca:
1. dbanie o bezpieczeństwo swojego systemu operacyjnego, ze szczególnym uwzględnieniem bieżących aktualizacji systemu, posiadania oprogramowania antywirusowego, antyspamowego itp.,
2. zainstalowanie zabezpieczeń przeciwprzepięciowych, zabezpieczających sprzęt komputerowy,
3. stosowanie do kont pocztowych oraz innych aplikacji internetowych wymagających podania hasła, haseł o długości co najmniej 8 znaków, zawierających oprócz małych i dużych liter także cyfry i inne znaki, w tym interpunkcyjne a także okresową zmianę haseł,

Prezes UKE publikuje na stronie internetowej UKE (www.uke.gov.pl) aktualne informacje o:

1. bezpieczeństwie komunikacji elektronicznej w cyberprzestrzeni – https://www.uke.gov.pl/bezpieczenstwo-komunikacji-elektronicznej-w-cyberprzestrzeni-15265.
2. bezpieczeństwie komunikacji elektronicznej w cyberprzestrzeni (urządzenia mobilne) - https://www.uke.gov.pl/bezpieczenstwo-komunikacji-elektronicznej-w-cyberprzestrzeni-urzadzenia-mobilne-17398.

Usługodawca zaleca zapoznanie się ze wskazanymi powyżej opracowaniami dotyczącymi bezpieczeństwa w cyberprzestrzeni.