INFORMACJA O SZCZEGÓLNYCH ZAGROŻENIACH ZWIĄZANYCH Z KORZYSTANIEM PRZEZ UŻYTKOWNIKÓW Z USŁUG ŚWIADCZONYCH DROGĄ ELEKTRONICZNĄ PRZEZ MICHAŁ PANKIEWICZ & WSPÓŁPRACOWNICY KANCELARIA PRAWNA

Michał Pankiewicz & Współpracownicy Kancelaria Prawna (dalej: „Usługodawca" lub „Kancelaria") wykonując obowiązek wynikający z art. 6 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r., nr 144, poz. 1204 z późn. zm.), informuje o szczególnych zagrożeniach związanych z korzystaniem przez użytkowników z Usług świadczonych przez Kancelarię drogą elektroniczną (dalej łącznie: „Usługobiorcy" lub pojedynczo „Usługobiorca").

Informacja dotyczy zagrożeń identyfikowanych jako zagrożenia potencjalne, które powinny być brane pod uwagę mimo stosowania przez Usługodawcę systemów zabezpieczających infrastrukturę przed nieuprawnionym oddziaływaniem osób trzecich.

Podstawowym zagrożeniem każdego użytkownika Internetu, w tym Usługobiorcy, jest:

1. możliwość „zainfekowania" systemu teleinformatycznego przez różnego rodzaju oprogramowanie tworzone głównie w celu wyrządzania szkód, typu wirusy, „robaki", malware czy „konie trojańskie",
2. możliwość otrzymania spamu, czyli niezamówionej informacji reklamowej (handlowej) przekazywanej drogą elektroniczną,
3. możliwość łamania zabezpieczeń w celu pozyskania osobistych i poufnych informacji w celu kradzieży tożsamości,
4. możliwość wyłudzania poufnych informacji osobistych np. haseł (phishing) poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne i w konsekwencji pozyskanie osobistych i poufnych informacji dotyczących Usługobiorcy,
5. możliwość zainstalowania programów śledzących działanie Usługobiorcy, przechwytywanie i ewentualne analizowanie danych przepływających w sieci (spyware).

Usługodawca informuje, że mimo stosowania rozmaitych, nowoczesnych technologii „obronnych" nie istnieje perfekcyjne zabezpieczenie chroniące przed opisanymi wyżej niepożądanymi działaniami.

W celu uniknięcia wskazanych zagrożeń Usługobiorca powinien:

1. zaopatrzyć swój komputer oraz inne urządzenia elektroniczne, które wykorzystuje podłączając się do sieci internet, w program antywirusowy,
2. stale aktualizować program antywirusowy, instalując jego najnowsze wersje, niezwłocznie po pojawieniu się ich na rynku,
3. dokonywać regularnych całościowych skanów systemu programem antywirusowym i antymalware,
4. instalować programy prewencyjne wykrywające i zapobiegające włamaniom,
5. używać oryginalnego systemu i aplikacji pochodzących tylko z legalnego źródła,
6. czytać wszelkie umowy licencyjne, regulaminy, itp.,
7. prawidłowo ustawić przeglądarkę internetową,
8. nie otwierać załączników poczty e-mail niewiadomego pochodzenia.

Ochronę przed zagrożeniami związanymi z korzystaniem przez Usługobiorców z usług świadczonych drogą elektroniczną zapewniają także: firewall tj. włączona zapora sieciowa, szyfrowanie transmisji danych, wyłączenie makr w plikach MS Office nieznanego pochodzenia. Konsekwentne stosowanie przez Usługobiorcę ze wskazanych powyżej środków bezpieczeństwa pozwala uniknąć potencjalnych niebezpieczeństw związanych z korzystaniem z internetu.

Zgodnie z art. 6 pkt 2 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r., nr 144, poz. 1204 z późn. zm.) Usługodawca informuje, że funkcja i cel oprogramowania lub danych niebędących składnikiem treści Usług, wprowadzanych przez Kancelarię do systemu teleinformatycznego, którym posługuje się Usługobiorca określone zostały w Polityce Prywatności.