Informacja o szczególnych zagrożeniach związanych z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną przez *AB - Tuning Tomasz Bródka z siedzibą w Knurowie*

AB - Tuning Tomasz Bródka z siedzibą w Knurowie, ul. Emilii Plater 39, 44-190 Knurów, REGON 276711490, NIP 969 0386096, wpisany do Centralnej Ewidencji i Informacji o Działalności Gospodarczej (dalej: *Właściciel Serwisu*) w wykonaniu obowiązku z art. 6 pkt 1) ustawy z dnia 18 lipca 2002 r. oświadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204 z późn. zm.), informuje o szczególnych zagrożeniach związanych z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną za pośrednictwem Serwisu internetowego www.bmwyprawy.pl

Informacja niniejsza ma na celu przedstawienie zagrożeń, które mogą wystąpić jedynie potencjalne, ale które powinny być brane pod uwagę, mimo stosowania przez Właściciela Serwisu środków zabezpieczających infrastrukturę Serwisu internetowego przed nieuprawnionym działaniem lub dostępem osób trzecich.

Do podstawowych zagrożeń związanych z korzystaniem z sieci Internet należą:

- złośliwe oprogramowanie (ang. *malware*) – mianem *malware* określa się wyłącznie oprogramowanie, które zostało przeznaczone do złych celów i działa wbrew oczekiwaniom użytkownika takie jak wirusy, robaki, trojany (konie trojańskie), keyloggery, dialery; określenie to nie obejmuje aplikacji, które mogą wyrządzić niezamierzoną szkodę z powodu jakiejś niedoskonałości;

- programy szpiegujące (ang. *spyware*) – oprogramowanie zbierające dane o osobie fizycznej lub prawnej bez jej zgody, mogą to być informacje o odwiedzanych stronach, dane dostępowe itp. Występuje często jako dodatkowy i ukryty komponent większego programu, odporny na usuwanie i ingerencję użytkownika. Programy szpiegujące mogą wykonywać działania bez wiedzy użytkownika – zmieniać wpisy w rejestrze systemu operacyjnego i ustawienia użytkownika. Program szpiegujący może pobierać i uruchamiać pliki pobrane z sieci;

- spam - niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym;

- wyłudzanie poufnych informacji osobistych (np. haseł) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. *phishing*);

- włamania do systemu teleinformatycznego użytkownika z użyciem m.in. takich narzędzi hackerskich jak *exploit* i *rootkit*.

Użytkownik, aby uniknąć powyższych zagrożeń, powinien zaopatrzyć swój komputer i inne urządzenia elektroniczne, które wykorzystuje podłączając się do Internetu, w program antywirusowy. Program taki winien być stale aktualizowany. Ochronę przed zagrożeniami związanymi z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną zapewniają także:

- włączona zapora sieciowa (ang. *firewall*),
- aktualizacja oprogramowania,
- nieotwieranie załączników poczty elektronicznej niewiadomego pochodzenia,
- czytanie okien instalacyjnych aplikacji, a także ich licencji,
- wyłączenie makr w plikach MS Office nieznanego pochodzenia,
- regularne całościowe skany systemu programem antywirusowym i antymalware,
- szyfrowanie transmisji danych,
- instalacja programów zapobiegających (wykrywania i zapobiegania włamaniom),
- używanie oryginalnego systemu i aplikacji, pochodzących z legalnego źródła.

Knurów,2019.06.12