

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

Cinema City Poland Sp. z o.o., wykonując obowiązek z art. 6 pkt 1) ustawy z dnia 18 lipca 2002 r. o świadczeniu 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.

Informacja niniejsza dotyczy zagrożeń, które mogą wystąpić jedynie potencjalnie, ale które powinny być brane pod uwagę, mimo stosowania przez Cinema City Poland Sp. z o.o. środków zabezpieczających infrastrukturę Cinema City Poland Sp. z o.o. przed nieuprawnionym działaniem osób trzecich.

Do podstawowych zagrożeń związanych z korzystaniem z sieci Internet należą:

- 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;
- programy szpiegujące (ang. *spyware*) - programy śledzące działania użytkownika, które gromadzą informacje o użytkowniku i wysyłają je - zazwyczaj bez jego wiedzy i zgody - autorowi programu;
- spam - niechciane i niezamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym;
- wyludzanie 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 wszelkiego 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 prewencyjnych (wykrywania i zapobiegania włamaniom), używanie oryginalnego systemu i aplikacji, pochodzących z legalnego źródła.