**aut. Tomasz Fastyn** 24.05.2016

# POLSKIE PLATFROMY SPRZEDAJĄCE GRY I ICH POZIOMY ZABEZPIECZEŃ

Zabezpieczenia w internecie nie dotyczą tylko stron czy aplikacji bankowych, ale również serwisów zajmujących się sprzedażą przedmiotów czy treści cyfrowych. Szczególnie ciekawy wydaje się polski rynek gier, który rozwija się bardzo dynamicznie. Sprawdziliśmy, jak zabezpieczone są portale zajmujące się dystrybucją gier online.

Segment gier jest jednym z najdynamiczniej rozwijających się branż. Według ostatnich danych światowy rynek szacowany jest na co najmniej 100 mld dolarów, polski na ok. 2 mld złotych. Większość firm oferuje możliwość rozgrywek online, zazwyczaj grę możemy też kupić w formie cyfrowej. Klienci nie muszą czekać, aż kurier dostarczą im pudełko z płytą - po prostu pobierają grę ze strony twórców.

Polskich firm sprzedających cyfrowe wersje gier na globalnych rynkach jest kilka. największe to GOG – spółka stworzona przez grupę CdProjekt, Kinguin oraz najmłodszy wśród nich GamesRepublic, którego współtwórcą jest warszawskie 11bit studios. Skontaktowaliśmy się z firmami i zapytaliśmy ich, jak wygląda kwestia cyberbezpieczeństwa podczas kupowania gry online.

Aktualnie na platformie Kinguin.net weryfikacja użytkownika odbywa się przez aktywowanie przez niego mechanizmu tzw. Two Factor Authentication - co oznacza wysłanie specjalnego kodu na maila, który trzeba wpisać po zalogowaniu się. Mechanizm uaktywnia się po wykryciu logowania z nowej przeglądarki lub adresu IP. W podobny sposób Steam zabezpiecza swoją aplikację oraz stronę WWW.

- Nasza platforma zabezpieczona jest przed atakami wymierzonymi w dane użytkowników oraz dostępność serwisu. Przed atakami typu DDOS chroni nas usługa wyspecjalizowana w analizie ruchu sieciowego na wszystkich warstwach, co pozwala na jej szybką adaptację oraz rozpoznawanie nieprawidłowości. Wykrywa ona zarówno zmasowany ruch skierowany w platformę, jak również spreparowane zapytania mające na celu spenetrowanie zabezpieczeń i konfiguracji aplikacji. Ataki typu Brute Force są skutecznie zatrzymywane poprzez zaimplementowany na logowaniu mechanizm reCaptcha, gdzie zaufaliśmy firmie Google w dostarczonym rozwiązaniu i nie zawiedliśmy się – mówi Maciej Mroziński z firmy Kinguin.

Portale sprzedające gry korzystają z różnych zabezpieczeń, ale raczej unikają korzystania z tokenów, które są popularne w bankowości elektronicznej.

- Nie posiadamy systemu zabezpieczeń tokenami. By zalogować się do swojego konta w serwisie Gamesrepublic wystarczy podać adres e-mailowy i hasło, które były podawane w trakcie zakładania konta. Nie stosujemy zaawansowanego zabezpieczenia konta użytkownika, gdyż z naszej strony nie pobieramy wrażliwych danych od użytkowników, poza ich adresami e-mail. Przy płatności za gry w Games Republic nie zapisujemy żadnych danych dotyczących kart płatniczych czy danych do kont PayPal, wszystko odbywa się poprzez szyfrowane transakcje internetowe, udostępnione przez naszych

partnerów od systemów płatności. Jest to na pewno krok, który może wpłynąć na poprawę bezpieczeństwa użytkowników - mówi Łukasz Kukawski z firmy Games Republic.

Już w tej chwili logując się do platformy Steam z nowego urządzenia, które nie zostało wcześniej zatwierdzone przez użytkownika, na adres e-mail danego konta jest wysyłany kod, który należy wprowadzić w aplikacji Steam. Czy dodatkowe wprowadzenie tokenów przy każdym logowaniu zapewni 100% bezpieczeństwo? Zapewne nie, gdyż hakerzy potrafią obejść każde możliwe zabezpieczenie, ale mogą one drastycznie zmniejszyć ilość kont przechwytywanych przez hakerów.

Jednak jest pewna różnica pomiędzy serwisem takim jak GamesRepublic.com, a serwisami Steam, Origin czy PlayStation Network.  - Games Republic to przede wszystkim sklep, w którym użytkownicy mogą kupić oryginalne gry na PC w olbrzymiej większości w postaci klucza, który następnie jest realizowany na innej platformie (jak Steam czy UPlay). Tak więc przejęcie hakerskie konta użytkownika w Games Republic, w którym nie ma żadnych wrażliwych danych a klucze do gier są w większości już "użyte", jest mniej niebezpieczne niż przejęcie konta na serwisie typu Steam czy PSN, w którym użytkownik ma bezpośredni dostęp do swojej biblioteki gier i taki atak może go pozbawić wszystkich swoich zakupów – dodaje Łukasz Kukawski.

**Czytaj też:** Telefony z obsługą biometrii wyznaczają trendy w dziedzinie zabezpieczeń