Cyberdefence 24

aut. Tomasz Fastyn 10.05.2016

WERYFIKACJA SMS NIE JEST BEZPIECZNA

Uwierzytelnienie przelewów tylko za pomocą telefonu jest bardzo ryzykowne - twierdzą eksperci od cyberbezpieczeństwa.Oprócz programu antywirusowego czy zapory sieciowej, warto pomyśleć o kilkustopniowej weryfikacji. Zastosowanie choćby weryfikacji dwustopniowej – za pomocą hasła i kodu SMS znacznie poprawia nasze bezpieczeństwo w sieci.

O lukach w obecnie stosowanych metodach weryfikacji logowania czy wykonywania przelewów, wiadomo choćby z ostatnich doniesień na temat protokołu SS7, który jest używany na całym świecie do przekazywania informacji między telefonami z różnych sieci telekomunikacyjnych. Powszechnie znana jest podatność tego protokołu na ataki. Dziennikarze amerykańskiej stacji CBS udowodnili ostatnio, że dzięki lukom w protokołach Signalling System No. 7 (SS7) hakerzy bez problemu mogą podsłuchiwać rozmowy niemal każdego. Wystarczy im jedynie numer telefonu ofiary.

Do tego problemu nawiązał Marcin Ludwiszewski z firmy Deloitte, który na konferencji „Współczesny napad na bank" podkreślał niewystarczający poziom zabezpieczeń, jaki oferuje autoryzacja sms. Jest to szczególnie ważne przy korzystaniu z mobilnych wersji aplikacji bankowych, w których cały proces weryfikacji i potwierdzania odbywa się na jednym urządzeniu.

Dlatego najlepszym rozwiązaniem jest korzystanie z niepowiązanych ze sobą elementów weryfikacji. Takich, które albo nie posiadają dostępu do sieci albo łączą się z nią tylko na chwilę w celu autoryzacji. Należy przy tym korzystać z dodatkowych źródeł zabezpieczeń. Programy bankowe lub komunikacyjne umożliwiają czasem korzystanie z takich opcji jak hasło, token, kod captcha, podpis elektroniczny czy zabezpieczenia biometryczne.

Zaszyfrowane hasła da się niekiedy złamać, wymaga to cierpliwości lub sprytu, zależy to wszystko od poziomu wiedzy hakera oraz urządzeń, których używa.

Tokeny, szczególnie tokeny sprzętowe niepodłączone do sieci wydają się bezpiecznym i najmniej obecnie narażonym na ataki rozwiązaniem. Są niepodłączone do sieci, nie ma możliwości ich zdalnego przejęcia.

Kod captcha jest dobrym rozwiązaniem, jednak nie do wszystkiego. Ogranicza ruch złośliwych botów i blokuje im dostęp do niektórych elementów stron. Jednak w sieci dostępne są programy rozwiązujące takie metody zabezpieczeń. Co więcej kody captcha od firmy Google są zwykle tworzone przez programy. Naasuwa się więc pytanie, czy coś co zostało stworzone przez program, może być złamane przez inny program?

Podpisy elektroniczne i zabezpieczenia biometryczne w bankowości to niestety ciągle nowość, ale wydają się krokiem, w którym będą zmierzać banki - sugeruje Marcin Ludwiszewski z Deloitte. Dlatego najlepiej zmienić swoje przyzwyczajenia w celu poprawy bezpieczeństwa swojej komunikacji i dostępu do konta.

Czytaj też: [Internetowi oszuści podszywają się pod InPost]