Media społecznościowe a bezpieczeństwo danych

Wydarzenia ostatnich dni, odnośnie bezpieczeństwa danych w mediach społecznościowych, pokazały, że ten aspekt korzystania z sieci musi być traktowany przez wszystkich użytkowników priorytetowo.

Gigantyczna ilość prywatnych danych, przechowywanych obecnie na serwerach, jest z jednej strony wystarczającą motywacją dla hackerów do zdobycia dostępu do tych danych, a z drugiej strony sporym wyzwaniem dla administratorów i działów bezpieczeństwa portali, aby te dane zabezpieczyć, przy zachowaniu wysokiej dostępności.

To nie wszystko. Bezpieczeństwo danych użytkowników korzystających z zasobów Internetu zależy również od poziomu ich świadomości nt. zagrożeń płynących z sieci podczas korzystania z niej.

Przypominamy kilka zasad, którymi należy się kierować, aby zminimalizować ryzyka związane z korzystaniem z mediów społecznościowych:

- stosować silne hasło – można w tym celu posłużyć się generatorem haseł;
- stosować dwuetapowe logowanie – najpierw podajemy login i hasło, a później potwierdzamy logowanie zewnętrznym tokenem. Zastosowanie takiego klucza sprzętowego skutecznie zabezpieczy przed atakami hakerskimi (phishingiem, przechwytywaniem sesji czy wyłudzeniem danych). Ponadto token nie zadziała podczas logowania na fałszywej stronie;
- nie logować się na nieznanych urządzeniach;
- stosować różne hasła do różnych portali i systemów, w czym może pomóc nam manager haseł;
- nie korzystać z niezaufanego połączenia internetowego (publiczne hot spoty);
- ograniczyć uprawnienia aplikacji do logowania za pomocą konta w portalu społecznościowego.

Co zrobić, gdy podejrzewamy, że nasze dane mogły wyciec?

- bezwzględnie należy, najszybciej jak to możliwe, zmienić hasło przy zachowaniu zasad tworzenia złożonego hasła;
- należy zachować szczególną ostrożność przed atakami phishingowymi. Ataki te mogą się nasilić po wycieku danych kontaktowych (e-mail). Pod żadnym pozorem nie używajmy odnośników znajdujących się w otrzymanej poczcie, w szczególności w korespondencji niezamówionej lub pochodzącej od nieznanych osób, instytucji i firm;
- należy zachować ostrożność przed atakami socjotechnicznymi, przeprowadzanymi przy użyciu telefonu. Potencjalny hacker może wykorzystać przechwycone z portalu społecznościowego dane, podczas na przykład rozmowy telefonicznej z ofiarą ataku uwierzytelnić się , a następnie zdobyć bezpośrednio dalsze informacje, w tym dostęp do systemów lub urządzeń użytkownika.