WYCIEK INFORMACJI FACEBOOKA. CZEKA NAS LAWINA ATAKÓW PHISINGOWYCH [KOMENTARZ EXATELA]

Informacja o potencjalnym ujawnieniu danych ponad 2 miliardów osób jest kolejnym z problemów, które w ostatnim czasie spadły na Facebooka. W tym przypadku warto zwrócić uwagę, że doszło do niego wykorzystując wbudowane mechanizmy. Chciałoby się wręcz napisać, że to nie błąd, to funkcjonalność. Wpisując adres e-mail lub numer telefonu można było poznać szereg podstawowych danych o użytkownikach

Przypomnijmy – najpierw miały miejsce bardzo poważne oskarżenia o świadomą pomoc przy dystrybuowaniu reklam mogących wpłynąć na wynik wyborów w USA. Ostatnio obserwowaliśmy ciąg dalszy historii z firmą Cambridge Analytisc w roli głównej. To skończyło się wezwaniem Marka Zuckerberga na przesłuchanie przez Kongres USA. Potem pojawiały się oskarżenia, że umieszczane na stronach skrypty Facebooka gromadzą informacje również o osobach, które nie są użytkownikami tej platformy. Teraz słyszymy o ujawnieniu przez firmę informacji o 2,2 miliarda kont. Jednocześnie obserwujemy ich oskarżenie przez Electronic Frontier Foundation o złe funkcjonowania algorytmów rozpoznawania twarzy (podobno rozpoznają i znakują również te osoby, które nie wyraziły na to zgody). A w tle mamy jeszcze rozstanie się w atmosferze wielu niedomówień Facebook'a z Alexem Stanosem – ich CSO (czyli szefem bezpieczeństwa).

Wracając do kwestii wycieku informacji o 2,2 miliarda kont. W tym przypadku warto zwrócić uwagę, że doszło do niego wykorzystując wbudowane mechanizmy. Chciałoby się wręcz napisać, że to nie błąd, to funkcjonalność. Wpisując adres e-mail lub numer telefonu można było poznać szereg podstawowych danych o użytkownikach. Wykorzystując wędrujące po sieci listy ponad miliarda skompromitowanych adresów e-miał przestępcy napisali skrypty weryfikujące ich obecność w tej sieci społecznościowej. I w olbrzymiej liczbie przypadków udało się je powiązać ze sobą. Co to oznacza? Przestępcy mają nie tylko informacje o adresie e-mail oraz wykorzystywanych hasłach, ale mogą je przypisać konkretnej osobie, poznać jej numer telefonu... To najprawdopodobniej doprowadzi do lawinowych ataków phishingowych. Może też ułatwić prace analityczne pozwalające lepiej rozpoznać potencjalne „cele". A jak się do tego doda informacje, które Facebook udostępniał Cambridge Analytics (i pewnie wielu innym firmom), to trudno dłużej mówić o jakiejkolwiek prywatności.

No dobrze, ale to już się stało. Co mają zrobić zwykli użytkownicy? No właśnie, niewiele… Mogą wykonać jedynie podstawowe czynności:

- zmienić hasła (i zmieniać je regularnie), najlepiej na długie i niepowtarzalne. Dobrze do tego nadają się programy typu menadżer haseł lub urządzenia typu U2F

- pilnować historię kredytową

- mieć poustawiane powiadomienia o zmianach haseł na różnych wykorzystywanych portalach

- zachowywać czujność czytając maile i stale kształcić się w zakresie nowych technik phishingowych

Najważniejsze jednak to zastanowić się nad dalszym sensem umieszczania historii swojego życia w mediach społecznościowych i możliwymi tego konsekwencjami.

Warto jednocześnie podkreślić, że w wyniku wychodzenia na jaw kolejnych „sensacyjnych doniesień" udało się dokonać w Facebooku zmian, na które od lat czekali obrońcy prywatności. Użytkownicy mogą zobaczyć, jakie aplikacje mają dostęp do danych. W końcu pojawiły się programy wyszukujące podmioty nadużywające zasad dostępu do danych. Ustawiono także maksymalny czas gromadzenie niektórych rodzajów informacji. Facebook poinformował także, że zwiększył zatrudnienie zespołów pilnujących kwestii prywatności z 10 000 do 20 000 pracowników… Możliwe, że zaraz pojawi się informacja o wdrożeniu nowych reguł, które ułatwią zidentyfikowanie ruchu z zapytaniami o dane osób na podstawie adresu e-mail.

Na zakończenie warto zauważyć, że powstała w ostatnim czasie nowa, świecka tradycja. Im bliżej do wejścia w życie rozporządzenia o ochronie danych osobowych tj. The General Data Protection Regulation (w skrócie GDPR), tym więcej organizacji „dowiaduje" się o wycieku danych. Trudno jednoznacznie stwierdzić, czy to skutek większej świadomości podmiotów w zakresie swojej odpowiedzialności czy strach przed nadchodzącymi karami. Wyraźnie widać pozytywny wpływ dyrektywy, która uniemożliwi „zamiatanie pod dywan" tego typu wypadków. To z pewnością doprowadzi do zwiększenia poziomu ochrony danych.

Podsumowując – duże międzynarodowe firmy są już świadome swoich obowiązków i odpowiedzialności związanej z gromadzeniem tego typu informacji. Badania dotyczące cyberbezpieczeństwa polskiego biznesu, które EXATEL przeprowadził w 2017 roku pokazują dobitnie, że świadomość wśród krajowych przedsiębiorców jest na znacznie niższym poziomie.

Autor: Jakub Syta - Dyrektor Departamentu Cyberbezpieczeństwa