W INTERNECIE NIE ISTNIEJE JUŻ POJĘCIE PRYWATNOŚCI

To dziwne uczucie, kiedy wydaje się nam, że jesteśmy śledzeni. Instynkt podpowiada, żeby sprawdzić, czy ktoś nas obserwuje. – W rzeczywistym świecie zachowujemy ostrożność, ale dlaczego nie robimy tego w Internecie? – na to pytanie odpowiada Maciej Aniserowicz, bloger programistyczny.

Co chwila miliony użytkowników zostawiają po sobie ślady na stronach internetowych. Kliknięcie w daną reklamę, otworzenie interesującego linku, a nawet wchodzenie na zaufane witryny – to wszystko jest rejestrowane najczęściej za naszą zgodą, jednak mało kto zdaje sobie z tego sprawę. I choć podświadomie można się tego domyślać, nie zaprzątamy sobie tym głowy i „scrollujemy" kolejne strony. Kiedy mówimy o zbieraniu danych w Internecie, najczęściej zakładamy, że chodzi o numery kart, adresy i maile. A co, jeśli strony wiedzą co lubimy i co nas interesuje? Prawdopodobnie każdy uniósł kiedyś brew w zdziwieniu widząc na tym czy innym portalu reklamę produktu. Produktu, który dopiero co oglądał w zupełnie innym, niezależnym sklepie internetowym. Ostatnio wiele mówi się o screenie strony niezalezna.pl zamieszczonym na Twitterze Tomasza Lisa. Opinia publiczna dyskutuje o tym, czy dziennikarz faktycznie wchodził na serwisy randkowe. To, że zobaczył na stronie akurat taki baner, jeszcze o niczym nie świadczy, ponieważ istnieją różne sposoby kierowania reklam. Jedną z nich jest tzw. retargeting – reklama wyświetla się osobom, które oglądały wcześniej konkretne towary. Reklamy mogą też pojawiać się na stronach powiązanych tematycznie lub wyłącznie odbiorcom, którzy zostali zdefiniowani w kampanii. Reklamodawca może też ustawić reklamę tak, aby wyświetlała się jak największej liczbie użytkowników, bez sprecyzowanych kryteriów.

Wiedza to potęga

Nie musimy być ofiarami ataku „hakerów", żeby nasze informacje dostały się w ręce, o których nawet nie wiemy. Wchodząc na przykład na czyjegoś Facebooka, niejeden „detektyw" może szybko stwierdzić, jakiej muzyki słuchamy, co jemy, gdzie się bawimy, z kim lub gdzie mieszkamy. I dzieje się tak, bo ktoś zapomniał kliknąć odpowiednią opcję w zakładce „prywatność". Co więcej, jest możliwe śledzenie również ruchu naszego kursora i historii przeglądarki, a stąd już niewielki krok do tego, żeby wiedzieć o nas wszystko.– *Zebrane informacje są kluczowe do efektywnego działania procesu sprzedaży i profesjonalnej interakcji z klientami. Dzięki dokładnemu profilowi każdego klienta, firmy są w stanie dostosować do niego swoją ofertę. Znając potrzeby i analizując trendy mogą próbować nam, klientom… dogodzić* – tłumaczy najpopularniejszy polski bloger programistyczny, Maciej Aniserowicz. Firmy, by lepiej funkcjonować, potrzebują jak najbardziej trafnych decyzji w swojej strategii. I to właśnie my dostarczamy im formacji, co lubimy, bądź czym się interesujemy. Blogerzy mogą na bieżąco sprawdzać, ile osób wchodzi na ich strony, w jakim są wieku i jak to się zmienia w skali roku. Przykładowo, klikając „zgodę na wykorzystanie cookies" pozwalamy na „śledzenie" naszych poczynań na danej stronie. W większości przypadków, pozostawiane dane pomagają innym lepiej wykonywać swoją pracę, choć nie zawsze...

Inną kwestią są działania hakerów. Każdy z nich może mieć zupełnie inny cel. – *Jedni chcą nas okraść.*

Inni – jak w serialu Mr. Robot – zbawić przed wszechwładnymi korporacjami. Jeszcze inni chcą dla własnej satysfakcji złamać zabezpieczenia, których nikt wcześniej nie złamał – mówi Maciej Aniserowicz. Trzeba też pamiętać o złośliwym oprogramowaniu. W tej kwestii istnieje prawdziwy wachlarz możliwości: od zapisywania każdego kliknięcia na klawiaturze w celu wykradania np. haseł, po podglądanie przez kamery internetowe czy zbieranie danych z dysku komputera.

Samoobrona internetowa

W całym procesie zbierania informacji bardzo niebezpieczna jest niska świadomość użytkowników Internetu o tym, co dzieje się z ich danymi.Bezpiecznie jest założyć, że anonimowość w Internecie zniknęła i nigdy nie wróci. Więc co możemy zrobić, żeby ograniczyć dostęp do naszych danych? Ważne są hasła i ich siła. Porządny klucz powinien być długi i niemożliwy do zapamiętania dla nikogo, włączając w to nas samych. – *Dobrą metodą jest wygenerowanie takiego hasła programem typu menadżer haseł np. KeePass. Dodatkowo polecam korzystać z opcji autoryzacji dwustopniowej, którą proponuje wiele popularnych platform, jak Google czy Facebook. Po włączeniu tej opcji sama znajomość hasła nie wystarczy, żeby zalogować się na konto. Trzeba dodatkowo wpisać treść SMS-a lub jednorazowy kod wygenerowany przez specjalną aplikację. Istotne są również sygnały przekazywane nam przez przeglądarki. Tutaj dwoma ważnymi skrótami są HTTPS oraz SSL. Strony oferujące komunikację z wykorzystaniem tych zabezpieczeń oznakowane są przez przeglądarki charakterystyczną kłódeczką na zielonym tle. Korzystając z takich stron możemy założyć, że prawdopodobnie nikt – oprócz ich właścicieli – nie jest w stanie „podejrzeć" tego, co na nich robimy* – tłumaczy Maciej Aniserowicz. Możemy także spróbować ograniczyć ilość informacji, jakie każda strona internetowa posiada na nasz temat, włączając funkcję „anonimowego przeglądania Internetu", dostępną w każdej przeglądarce. Nazywa się to „incognito mode" lub „private browsing". Otwarcie nowej karty przeglądarki w takim trybie spowoduje, że odwiedzane strony nie będą mogły sięgnąć do naszej internetowej historii. A dane zapisane przez nie na naszym komputerze, zostaną automatycznie skasowane po zamknięciu przeglądarki. Jest to jednak dosyć prymitywny mechanizm i nie oznacza oczywiście, że naprawdę stajemy się wtedy anonimowi w sieci. – *Trzeba pamiętać też o tym, że gdy udostępnimy coś w Internecie, to zostanie tam już na zawsze* – podsumowuje Maciej Aniserowicz.

Maciej Aniserowicz – jeden z najpopularniejszych blogerów programistycznych w Polsce. Autor najpopularniejszego dev-bloga: devstyle.pl. Twórca podcasta programistycznego: DevTalk. Prelegent na największych polskich konferencjach oraz grupach pasjonackich w całym kraju. Jeden z liderów Białostockiej Grupy .NET oraz współorganizator konferencji Programistok.

Żródło: synertime.pl

Czytaj też: Powstaję globalny system kontroli i oceniania oprogramowania