

Jak tworzyć strony przyjazne prywatności użytkowników

22 grudnia 2014

Publikowanie treści w Internecie jest nieodłącznym elementem funkcjonowania we współczesnym świecie. Własna strona internetowa jest standardem w przypadku firm, instytucji publicznych czy organizacji. Przybywa też osób, które decydują się na komunikację z otoczeniem za pomocą właśnie tego medium. Koncentrując się na dotarciu do odbiorców, łatwo zapomnieć o tym, że funkcjonowanie strony internetowej wiąże się z szeregiem złożonych zagadnień technicznych, które mają realne konsekwencje dla prywatności odbiorców.

To, że w Internecie każdy nasz ruch jest śledzony, wynika z konkretnych rozwiązań technicznych proponowanych przez tworzące je firmy i wybieranych przez webmasterów. Narzędziem służącym do uświadomienia użytkownikom skali problemu jest wtyczka [Lightbeam](#) dla przeglądarki Firefox, rozwijana przez fundację Mozilla. Pokazuje ona, jakie serwery rejestrują naszą aktywność w Internecie podczas codziennego przeglądania stron. Kilka godzin korzystania z przeglądarki z włączonym Lightbeamem pozwala zorientować się, w ile zaskakujących miejsc trafiają informacje o nas.

Na jakie rozwiązania warto zwrócić uwagę przy tworzeniu i administrowaniu stroną internetową, by szanować prywatność użytkowników? Oto kilka kwestii, o których warto pamiętać.

NARZĘDZIA ANALIZY RUCHU

Mechanizmy pozwalające analizować ruch na stronie internetowej są przydatnym narzędziem z repertuaru każdego webmastera – pewna doza informacji o użytkownikach jest niezbędna, by zrozumieć, w jaki sposób korzystają oni ze zgromadzonych informacji. Pomaga to dostosować portale do potrzeb i oczekiwań odbiorców. W ostatnim czasie tradycyjne,

kontrolowane przez webmastera narzędzia do analizy ruchu ustępują miejsca rozwiązaniom SaaS (ang. Software as a Service). Nie jest to przypadek – rozwiązania te często dostarczane są za darmo i kuszą wygodą polegającą na braku konieczności instalacji oprogramowania – wystarczy wkleić fragment śledzący w kod strony. Przykładem takiego rozwiązania jest popularne narzędzie Google Analytics. Korzyści dla usługodawcy wynikające z rozpowszechnienia tego darmowego narzędzia są niekwestionowane – system zbierający dane o użytkownikach strony działa na jego serwerach i wszystkie statystyki pozostają pod jego kontrolą. Dodatkowo informacje uzyskane za pomocą naszej strony są łączone z danymi zebranymi z innych stron internetowych korzystających z danego rozwiązania i służą śledzeniu nawyków internautów oraz tworzeniu ich profili dla reklamodawców – to istota modelu biznesowego dostawców takich rozwiązań. Jak widać, użytkownicy portali często płacą ukrytą cenę za wygodę webmastera.

Alternatywą dla rozwiązań SaaS jest stosowanie oprogramowania, które można samodzielnie zainstalować i kontrolować. Istnieje wybór narzędzi służących zbieraniu i analizie statystyk stron internetowych, często są one udostępniane jako wolne oprogramowanie. Jednym z najpopularniejszych tego typu rozwiązań jest [Piwik](#), zbliżony w obsłudze do rozwiązań SaaS, jednak dający kontrolę nad zbieranymi danymi. Jego instalacja sprowadza się do uruchomienia dodatkowej strony internetowej i wklejenia fragmentu śledzącego w kod portalu, którego ruch chcemy analizować. Za pomocą tego narzędzia można zbierać informacje z wielu stron. Dodatkową zaletą Piwika jest respektowanie ustawień „Nie śledź” (ang. Do not track). Jest to dostępne w przeglądarkach internetowych ustawienie, które pozwala wysyłać stronom internetowym informację, że użytkownik nie życzy sobie zbierania jakichkolwiek informacji o swojej aktywności w Internecie. Włączenie tej opcji może zmniejszyć liczbę wyświetlanych przez narzędzie wizyt, jednak dane zbierane od „chętnych” użytkowników są w zupełności wystarczające na potrzeby standardowej analizy ruchu.

WTYCZKI PORTALI SPOŁECZNOŚCIOWYCH

Narzędzia SaaS do analizy ruchu nie są jedynym mechanizmem umożliwiającym udostępnianie informacji o użytkownikach strony zewnętrznym podmiotom i ich profilowanie na masową skalę. Na podobnej zasadzie działają wtyczki portali społecznościowych umożliwiające „lajkowanie”, dzielenie się treścią ze znajomymi lub dodawanie komentarzy. Wejście na stronę, na której znajduje się facebookowy przycisk „Lubię to” (lub podobny), automatycznie powoduje wysłanie informacji o takim zdarzeniu na serwer portalu społecznościowego. Tego typu dodatki są bardzo powszechne, m.in. na blogach i stronach serwisów informacyjnych, co zwiększa ilość informacji o tym, co czytamy i oglądamy, dostępnych dla korporacji i sprawia, że nasz profil jest bardziej kompletny. Co więcej – dzięki ciasteczkom (i innym podobnym mechanizmom) nie musimy być wcale zalogowani do śledzącej nas strony, żeby informacje o naszej aktywności zostały związane z odpowiednim profilem.

W obliczu problemu powszechnego śledzenia użytkowników za pomocą wtyczek społecznościowych zachęcamy webmasterów do rezygnacji z tych elementów. Zdajemy sobie jednak sprawę, że w przypadku wielu portali będzie to rozwiązanie trudne do zaakceptowania. W takim przypadku polecamy zastąpienie domyślnych dodatków wtyczką [Social Share Privacy](#). Pozwala ona na korzystanie z przycisków społecznościowych w sposób sprzyjający poszanowaniu prywatności użytkowników – informacje o wejściu na stronę z wtyczką nie są przesyłane aż do momentu, kiedy użytkownik postanowi „polubić” stronę lub podzielić się treścią ze znajomymi.

ZEWNĘTRZNE NARZĘDZIA HOSTINGOWE

Istnieje całe spektrum narzędzi odpowiedzialnych za śledzenie internautów bez ich wiedzy i zgody. Należą do nich m.in. systemy CDN (ang. Content Delivery Network) – zewnętrzne hostingi oraz portale wymiany plików. Niewiele osób zdaje sobie sprawę z tego, jak często podczas korzystania z

Internetu nieświadomie pobiera elementy od „trzeciej strony”. Ci, którzy nie godzą się na to lub po prostu nie ufają zewnętrznym dostawcom, mają niewielkie możliwości manewru – mogą jedynie zablokować zapytania do ich serwerów za pomocą dodatków do przeglądarki, co najczęściej sprawia, że strona, z której próbują skorzystać, przestaje działać lub być czytelna.

Przykład ten pokazuje, jak istotne są decyzje podejmowane w imieniu użytkowników stron przez ich twórców. Rozwiązaniem tego problemu jest po prostu serwowanie dodatkowych elementów (m.in. skryptów i czcionek) z naszego serwera, a nie zdawanie się na zewnętrzny hosting. Zamiast wrzucać zdjęcia i dokumenty na dysk wirtualny można umieścić je na własnym serwerze lub skorzystać z mechanizmów wbudowanych w naszego bloga lub CMS. Ten prosty ruch znacząco zwiększy kontrolę naszych gości nad informacjami, które są o nich udostępniane.

Znacznie bardziej złożonym problemem jest udostępnianie filmów – zwykle ze względu na duży rozmiar plików wideo. Jeśli limit transferu w naszym pakiecie hostingowym nie jest problemem, możemy zamieścić film bezpośrednio na naszej stronie za pomocą standardowego znacznika video w HTML5 (można skorzystać z rozwiązania [Video for Everybody](#)). Innym rozwiązaniem są niezależne platformy do udostępniania wideo takie jak [MediaGoblin](#). Niestety, w przypadku, kiedy limit transferu jest ograniczeniem, nie pozostaje nam obecnie nic innego jak skorzystać z jednej z zewnętrznych platform, takich jak np. Vimeo czy YouTube. W przypadku tej drugiej zalecamy skorzystać z opcji nocookie (można ją znaleźć w ustawieniach kodów embed), która wyłącza serwowanie ciasteczek śledzących oglądającym.

Autorstwo” Michał „Czesiek” Czyżewski, Małgorzata Szumańska
Źródło: [Fundacja Panoptikon](#)