FUNDACJA PANOPTYKON

Warszawa, 20 kwietnia 2016 r.

Stanowisko Fundacji Panoptykon w sprawie ochrony prywatności użytkowników stron internetowych instytucji publicznych

Obecnie standardem jest, że instytucja publiczna prowadzi stronę internetową, na której informuje o swojej działalności. Strony te często stanowią uzupełnienie dla Biuletynów Informacji Publicznej, które zobowiązane są prowadzić podmioty wykonujące zadania publiczne. Treści i układ Biuletynów, jak również dostępność stron dla osób z niepełnosprawnościami (standard WCAG) stanowi przedmiot zainteresowania obywateli i organizacji pozarządowych zajmujących się jawnością życia publicznego oraz prawami osób z niepełnosprawnościami. Dotychczas pomijanym zagadnieniem była natomiast potrzeba dbania przez instytucje publiczne – występujące w roli administratorów stron internetowych – o zapewnienie wysokiego standardu ochrony prywatności użytkowników ich stron.

W ramach szerszego projektu „Państwo a biznes nadzoru. Monitoring praktyk instytucji publicznych”[1], poświęconego komercyjnym narzędziom nadzoru, nabywanym i wykorzystywanym przez instytucje publiczne, Fundacja Panoptykon przyglądała się rozwiązaniom technicznym wybieranym przez instytucje publiczne na ich stronach internetowych. Interesowało nas nie tylko to, z jakich narzędzi do zbierania informacji o użytkownikach swoich stron korzystają instytucje, ale także to, z jakimi podmiotami dzielą się wiedzą o nich. Z tego względu przeanalizowaliśmy strony internetowe 70 różnych instytucji publicznych. Za pomocą dodatków do przeglądarki internetowej: Lightbeam (dostępny dla przeglądarki Mozilla Firefox) oraz Disconnect i Ghostery przetestowaliśmy strony wszystkich ministerstw, policji i innych służb, wszystkich miast wojewódzkich i kilku powiatowych (konkretnie strony urzędów miast i lokalnych zakładów komunikacji), Zakładu Ubezpieczeń Społecznych (ZUS) i Narodowego Funduszu Zdrowia (NFZ) – w tym ich oddziałów – oraz Generalnego Inspektora Ochrony Danych Osobowych (GIODO). W przypadku ministerstw dodatkowo przeanalizowaliśmy dostępne na stronach polityki prywatności.

Na podstawie zebranych informacji zwracamy uwagę na kilka problemów dotyczących ochrony prywatności użytkowników, które zaobserwowaliśmy:

1. Narzędzia analizy ruchu

Mechanizmy pozwalające analizować ruch na stronie internetowej są przydatnym narzędziem dla każdego administratora – pewien zasób informacji o użytkownikach jest niezbędny, by zrozumieć, w jaki sposób korzystają oni ze zgromadzonych informacji. Pomaga to dostosować portale internetowe do potrzeb i oczekiwań odbiorców. W ostatnim czasie tradycyjne, kontrolowane przez administratorów narzędzia do analizy ruchu ustępują miejsca rozwiązaniom SaaS (ang. *Software as a Service*). Rozwiązania te często dostarczane są

[1] Realizacja projektu współfinansowana była ze środków Europejskiego Obszaru Gospodarczego w ramach programu „Obywatele dla demokracji” oraz dzięki wsparciu Open Society Foundations.

bezpłatnie, a do ich funkcjonowania wystarczające jest wklejenie fragmentu śledzącego w kod strony, co może zachęcać do ich stosowania.

Przykładem takiego rozwiązania jest popularne narzędzie Google Analytics, z którego korzysta znaczna część instytucji. Informacje na ten temat można znaleźć przynajmniej w części polityk prywatności, jak również można się o tym przekonać dzięki dodatkom do przeglądarek blokującym elementy śledzące (np. Disconnect, Ghostery) lub pokazującym, z jakich innych serwerów jest zaciągana zawartość na danej stronie (Lightbeam).

Korzyści dla podmiotu rozpowszechniającego takie darmowe 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 stron instytucji publicznych 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. Pokazuje to, że informacje o użytkownikach są ceną, jaką płacą administratorzy stron wykorzystujących rozwiązania takie jak Google Analytics za wykorzystywanie zdawałoby się darmowego rozwiązania.

By zwiększyć dbałość o prywatność użytkowników administratorzy stron internetowych instytucji publicznych mogą sięgnąć po alternatywne dla SaaS rozwiązanie. Jest nim stosowanie oprogramowania, które można samodzielnie zainstalować i kontrolować zbierane za jego pomocą dane. 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 wspomnianych wyżej rozwiązań SaaS. Jego instalacja sprowadza się do uruchomienia dodatkowej strony internetowej i wklejenia fragmentu śledzącego w kod portalu, którego ruch ma podlegać analizie. 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 użytkowników, którzy nie korzystają z opcji „Nie śledź" są w zupełności wystarczające na potrzeby standardowej analizy ruchu.

2. Wtyczki portali społecznościowych

Posiadanie przez instytucje publiczne profili w serwisach społecznościowych samo w sobie budzi kontrowersje, w szczególności jeśli stają się one dominującym narzędziem komunikacji danej instytucji, co prowadzić może do dyskryminacji osób, które nie mają lub nie chcą posiadać kont w serwisach społecznościowych. Kolejny problem pojawia się, gdy na stronach instytucji publicznych działają wtyczki portali społecznościowych (Facebooka, Twittera, Google+), które bezpośrednio na stronie instytucji pozwalają na „polubienie" lub udostępnienie konkretnego materiału na profilu użytkownika w portalu społecznościowym. Niektóre instytucje wyświetlają na swojej stronie internetowej treści pojawiające się na profilu tej instytucji na konkretnym portalu społecznościowym. Wtyczki portali społecznościowych często nie są widoczne na głównej stronie, jednak po przejściu np. do zakładki z aktualnościami lub do konkretnej informacji można z łatwością zauważyć ich obecność.

Jeśli podmioty o charakterze publicznym sięgają po wtyczki i dodatki łączące ich strony z zewnętrznymi serwisami, to dzielą się z nimi informacjami o sposobie korzystania z danej strony przez użytkowników, a tych ostatnich (o ile nie włączą oni odpowiednich blokad) zmuszają do akceptowania polityk prywatności komercyjnych podmiotów, z którymi mogą nie chcieć mieć do czynienia. Gdy na stronie instytucji publicznej pojawia się wtyczka serwisu społecznościowego, dostaje on dane o tym, co czytał użytkownik czy jak wiele czasu spędził na danej stronie. Wzbogaca to informacje o osobie, którymi dysponuje prywatny podmiot (Facebook, Google czy Twitter). Osoby korzystające z serwisów społecznościowych, publikujące w nich treści zazwyczaj są świadome tego, że dzielą z nim wiedzą o sobie. Natomiast osoby korzystające ze strony instytucji publicznych, w szczególności te niemające kont w serwisach społecznościowych, mogą nie zdawać sobie sprawy z tego, że już przez samą ich obecność na stronie z wtyczkami, informacje o nich przekazywane są do serwisów społecznościowych.

Ze względu na śledzący charakter wtyczek portali społecznościowych zachęcamy do rezygnacji z umieszczania takich elementów na stronach instytucji publicznych. Alternatywą dla korzystania z wtyczek społecznościowych może być podlinkowanie na stronie internetowej profilu instytucji na portalu społecznościowym. Takie rozwiązania nie umożliwia podzielenia się informacją na portalu społecznościowym za pośrednictwem strony internetowej instytucji publicznej, jednak pozwala poinformować odbiorców, że instytucja taki profil posiada. Jeśli takie rozwiązanie jest nie do przyjęcia, polecamy zastąpienie domyślnych dodatków wtyczką Social Share Privacy. Pozwala ona na korzystanie z przycisków społecznościowych, jednak informacje o wejściu na stronę z wtyczką nie są przesyłane do komercyjnego serwisu aż do momentu, kiedy użytkownik postanowi „polubić" stronę lub podzielić się treścią ze znajomymi w tym serwisie. Rozwiązanie takie gwarantuje minimalny poziom poszanowania prywatności użytkowników i pozwala im na podjęcie decyzji o przekazaniu informacji o ich aktywności podmiotowi trzeciemu.

3. Inne kontrowersyjne rozwiązania

Efekt w postaci przekazywania zewnętrznemu komercyjnemu podmiotowi informacji o zainteresowaniach użytkownika ma miejsce się także wtedy, gdy na danej stronie internetowej zainstalowana jest aplikacja, np. Google Ajax Search, która pełni rolę wewnętrznej wyszukiwarki. Wpisując zapytanie w okno wyszukiwarki na stronie, w rzeczywistości korzystamy z wyszukiwarki firmy dostarczającej konkretne rozwiązanie, która otrzymuje informację o np. o numerze IP użytkownika, treści i czasie zapytania. Pozbawia to użytkownika możliwości wyboru wyszukiwarki, choćby takiej, która zbiera mniej informacji o użytkownikach.

Stosunkowo rzadko instytucje publiczne wykorzystują wtyczki o charakterze marketingowym, które pozwalają na określenie, jakie treści wyświetlone zostaną odbiorcom z konkretnego obszaru, czy na dopasowanie do nich reklam. Przykładem tego jest wykorzystywanie przez niektóre instytucje wtyczki o nazwie DoubleClick. Cześć komunikatów (np. ostrzeżenia o zagrożeniach czy informacje, gdzie szukać pomocy) przygotowywanych przez instytucje zapewne skierowana jest do osób przebywających na określonych terytorium. Możliwość geograficznego sprofilowania komunikacji w niektórych przypadkach może mieć uzasadnienie, jednak powinno być poprzedzone rozeznaniem dostępnych rozwiązań, by wybrać te, które zbierają i przekazują podmiotom trzecim możliwie mało danych o użytkownikach strony internetowej.

4. Informacje dla użytkowników strony internetowej

Odnosząc się do kwestii poszanowania przez administratorów stron internetowych instytucji publicznych prawa do prywatności użytkowników tych stron, warto zwrócić również uwagę na treść polityk prywatności. Dokumenty te powinny zawierać informacje o tym, jakie dane o użytkownikach zbiera strona, w jaki sposób dane będą wykorzystywane i komu będą udostępniane. W przypadku wykorzystywania rozwiązań komercyjnych, które wiążą się z przekazywaniem danych do innego podmiotu, powinno to być wyraźnie zaznaczone. Bardzo istotny jest wykorzystywany w politykach prywatności język – powinien być on przystępny dla każdego użytkownika strony, umożliwiając mu zrozumienie, jakie dane o nim są zbierane i ewentualnie przekazywane podmiotom trzeci.

Dobrą praktyką w zakresie treści polityk prywatności na stronach instytucji publicznych jest podawanie listy wykorzystywanych ciasteczek wraz z informacją o ich funkcji (przykładem takiego działania może być polityka prywatność na stronie Generalnego Inspektora Ochrony Danych Osobowych[2] czy Narodowego Funduszu Zdrowia[3]), co sprzyja przejrzystości działania. Jak również informowanie użytkowników o tym, w jaki sposób mogą podnieść poziom bezpieczeństwa i ochrony swoich danych, np. wskazując, jak zmienić ustawienia prywatności w najpopularniejszych wyszukiwarkach bądź odsyłając do zewnętrznych stron z takimi informacjami. Takie podejście nie rozwiązuje wszystkich problemów i nie zwalania administratora strony z podjęcia działań na rzecz ograniczenia zbierania i przekazywania podmiotom trzecim informacji o użytkownikach, jednak sprzyja podnoszeniu świadomości tych ostatnich. Jako przykłady tego typu praktyki można wskazać politykę prywatności na stronie internetowej Ministerstwa Cyfryzacji[4] czy urzędu gminy Radzymin[5].

* * *

W związku z powyższym zachęcamy administratorów stron internatowych instytucji publicznych do dokonania weryfikacji obecnie wykorzystywanych rozwiązań i wdrożenie takich, które w większym stopniu zapewniają poszanowanie prywatności użytkowników.

[2] Polityka prywatności i wykorzystywania plików cookies w serwisach internetowych GIODO, http://giodo.gov.pl/493/id_art/1026/j/pl/.

[3] Polityka prywatności i cookies serwisu internetowego Narodowego Funduszu Zdrowia, http://www.nfz.gov.pl/polityka-cookies/.

[4] Polityka prywatności serwisu internetowego Ministerstwa Cyfryzacji https://mc.gov.pl/polityka-prywatnosci.

[5] Polityka prywatności samorządowego portalu informacyjnego miasta i gminy Radzymin, http://www.radzymin.pl/asp/pl_start.asp?typ=14&sub=294&menu=395&strona=1.