**Kraków, 22.10.2018r.**

# Największa polska firma hostingowa chroni prywatność użytkowników, wprowadzając standard DNS over TLS

**Ilu osobom udostępnilibyście historię swojej przeglądarki? Niestety robicie to codziennie, nie mając tego świadomości. O tym jak ważna jest prywatność w sieci przypomina retoryczne pytanie skierowane do Marka Zuckerberga przez senatora Richarda Durbina - zapytał on, czy właściciel Facebooka podzieli się z wszystkimi nazwą hotelu, w którym przebywa?**

Niestety, o ile Zuckerberg nie musiał dzielić się informacją na temat swojego tymczasowego pobytu, tak przeciętny użytkownik Internetu codziennie dostarcza swoim operatorom historię każdego swojego kliknięcia. Nazwa.pl mówi temu stop i wprowadza dla 600 000 domen swoich klientów obsługę standardu DNS over TLS na serwerach DNS Anycast, który uniemożliwia podglądanie tego, co użytkownicy robą w Internecie.

Wszystko, co łączy się z przebywaniem online zaczyna się od wywołania serwerów DNS. Usługi DNS zazwyczaj dostarczane są przez operatorów internetowych i służą do tego, by w dużym uproszczeniu zamienić przykładowy adres www.nazwa.pl na numer IP, czyli ciąg cyfr 85.128.128.36, dzięki temu przeglądarka wie, do jakiego miejsca w sieci powinna zabrać użytkownika. System tłumaczenia nazw domen na cyfry jest już dość leciwy i bardzo słabo zabezpieczony. – *dziury w systemie wykorzystują między innymi dostawcy łącz internetowych, pozyskując wiedzę na temat tego, jaki serwis odwiedził dany użytkownik, nawet jeżeli sama wyświetlana treść jest szyfrowana. Informacje te mogą posłużyć na przykład do pozycjonowania treści reklamowych. Nazwa.pl jako pierwsza firma w Polsce wprowadziła zabezpieczenia, które uniemożliwiają inwigilację zapytań do DNS, a tym samym gwarantują prywatność wszystkim swoim Klientom* – mówi Krzysztof Cebrat, prezes zarządu nazwa.pl.

Problem braku prywatności został rozwiązany poprzez wprowadzenie szyfrowanego połączenia pomiędzy komputerem a serwerem DNS, na podobnej zasadzie jak ma to miejsce w przypadku szyfrowania transmisji stron WWW zabezpieczonych przy użyciu certyfikatów SSL. W tym miejscu warto jednak wyjaśnić, że DNS over TLS chroni prywatność przesyłanych zapytań i odpowiedzi z systemu DNS. Weryfikacją poprawności przesyłanych danych zajmuje się inne zabezpieczenie, czyli DNSSEC, którym to nazwa.pl pokrywa 90% wszystkich zabezpieczonych nim polskich domen.

- *Stosowanie równocześnie DNSSEC i DNS over TLS stanowi duże wyzwanie technologiczne dla firm hostingowych, dlatego tylko nieliczne z nich decydują się na wprowadzenie bezpiecznych rozwiązań dla swoich Klientów, mimo oczywistych korzyści płynących z rozwiązania* – mówi Krzysztof Cebrat, prezes zarządu nazwa.pl.

Dla przeciętnego użytkownika największą wartością dodaną wynikającą z wdrożenia tej technologii jest realne zwiększenie bezpieczeństwa. Synergia obu rozwiązań uniemożliwia przekierowanie ruchu DNS i zamianę docelowych treści podczas tego procesu. Rozwiązanie to odeśle ataki phishingowe do lamusa, przynajmniej w przypadku domen pochodzących z nazwa.pl.