**Kraków, 03.09.2018r.**

**TLS 1.3 debiutuje w Polsce na masową skalę**

**Najnowszy protokół bezpieczeństwa TLS 1.3 - Transport Layer Security, będący rozwinięciem** [**protokołu**](https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_internetowy)**SSL, został wdrożony na masową skalę przez nazwa.pl. Rozwiązanie to jest również wdrażane przez światowych gigantów technologicznych, takich jak Google czy Facebook. Zapewnia ono ochronę wychodzącego i przychodzącego ruchu oraz daje gwarancję, że informacje zostały przesłane w niezmodyfikowanej formie. Działanie TLS 1.3 sprowadza się w skrócie do tego, że dane internautów są po prostu bezpieczne.**

Rozwiązanie TLS 1.3 wdrażane jest przez światowych liderów technologicznych takich jak Cloudflare, Google i Facebook - rozpoczęli oni już implementację protokołu na swoich serwerach. Według badań, w połowie sierpnia 2018 roku około 5% połączeń Firefoksa odbywało się poprzez TLS 1.3, podobne wartości raportuje firma Cloudflare, Facebook także jest w trakcie wdrażania tego protokołu[[1]](#endnote-1). Wyznaczony przez IETF - Internet Engineering Task Force standard TLS 1.3, oznaczany także jako RFC8446, jest szybszy i odporniejszy na ataki z zewnątrz niż wcześniejsza jego wersja. Rozwiązanie jest już wspierane przez Firefox w wersji 61, a kolejne przeglądarki także niebawem będą go stosowały.

- *Bezpieczeństwo i stabilność w strefie domeny .pl jest dla NASK najwyższym priorytetem. Cieszę się, że nasz Partner - nazwa.pl - aktywnie działa w tym obszarze. W pierwszym kwartale zabezpieczył prawie 450 tys. nazw domen  protokołem DNSSEC, a teraz podniósł poziom bezpieczeństwa w domenie .pl poprzez wdrożenie najnowszego standardu TLS 1.3. Należy zaznaczyć, że beneficjentami obu tych zabezpieczeń są użytkownicy Internetu* - Krzysztof Olesik, Kierownik Zespołu Technicznej Obsługi Domen NASK PIB.

Jak wynika z badań firmy, przeprowadzonych na bazie klientów usług hostingowych w nazwa.pl, obecnie w Polsce 13,10% ruchu odbywa się za pomocą najnowszego protokołu, a liczba ta z dnia na dzień rośnie. Najpopularniejszą wersją zabezpieczenia jest obecnie TLS 1.2, z którego korzysta 85% urządzeń. Jednak, jak przewidują analitycy firmy, do końca roku więcej niż połowa połączeń do stron w nazwa.pl będzie odbywała się z wykorzystaniem TLS 1.3. Wprowadzenie rozwiązania TLS 1.3 to kolejny krok nazwa.pl w stronę poprawy bezpieczeństwa polskiego Internetu.

*- Standardy są po to, aby je wdrażać, szczególnie te dotyczące bezpieczeństwa. Dlatego czołowe przeglądarki i światowi gracze, tacy jak Google czy Facebook wspierają kolejne wersje zabezpieczeń, w tym protokół TLS 1.3. Nazwa.pl jako lider technologiczny branży hostingowej i rejestracji domen w Polsce również udostępnia najnowsze rozwiązania swoim Klientom. Bezpieczna domena i bezpieczny hosting to dziś standard, który wyznaczamy* – tłumaczy Krzysztof Cebrat, prezes zarządu nazwa.pl

W lipcu 2018r nazwa.pl udostępniła za darmo certyfikaty SSL dla domen zarejestrowanych w spółce i obsługuje obecnie około 600 tys. stron zabezpieczonych przez SSL/TLS. Badanie przeprowadzone przez top100.wht.pl na próbie ponad 2,5mln domen wskazuje, że certyfikaty SSL dostarczone przez nazwa.pl zabezpieczają ponad 60% wszystkich stron WWW funkcjonujących w Polsce, kolejne 20% zabezpieczają certyfikaty Let’s Encrypt, a resztę rynku dzielą pozostali usługodawcy. Dostarczenie tak dużej liczby certyfikatów SSL przez nazwa.pl to dosyć istotna informacja z uwagi na fakt, że do poprawnego działania nowoczesnego protokołu HTTP/2 przyspieszającego wczytywanie stron WWW konieczne jest nawiązywanie bezpiecznych połączeń SSL/TLS, które do poprawnego działania wymagają certyfikatów SSL zgodnych z nazwami domen które chronią. Masowe wdrożenie certyfikatów SSL przez nazwa.pl oznacza, że udział w wykorzystaniu nowoczesnego protokołu HTTP/2 oraz TLS 1.3 będzie proporcjonalny do ilości dostarczonych certyfikatów.

Zastosowanie dla każdego hostowanego serwisu WWW certyfikatów SSL, HTTP/2 i TLS 1.3 powoduje usprawnienia w zakresie bezpieczeństwa i szybkości działania stron WWW, tworząc wartość dodaną dla właścicieli stron WWW oraz ich Klientów.

1. <https://blog.mozilla.org/security/2018/08/13/tls-1-3-published-in-firefox-today/> [↑](#endnote-ref-1)