Bezpieczny duet, czyli kto nas chroni w Internecie

56% polskich internautów realizuje zakupy w sklepach internetowych. Do przewag e-commerce w postaci wygody, atrakcyjnych cen czy dużego wyboru produktów nie trzeba nikogo przekonywać. Fundamentalną kwestią jest również bezpieczeństwo internetowych transakcji, które muszą być zabezpieczone na wielu płaszczyznach. Kupujących chronią regulacje prawne, system bankowy, pośrednicy płatności, a także protokół sieciowy TLS wraz z certyfikatem SSL. Umożliwia on bezpieczną wymianę zaszyfrowanych danych pomiędzy sklepem a serwerem. Dlaczego warto z niego korzystać?

Badanie przeprowadzone przez top100.wht.pl na początku stycznia 2019 roku pokazuje, że aż 36% stron internetowych nie korzysta z bezpiecznego połączenia. To ryzykowne z perspektywy firm prowadzących m.in. sklepy internetowe i realizujących transakcje online. Brak ochrony danych klientów może mieć również poważne konsekwencje prawne. W dodatku przeglądarka Google Chrome standardowo oznacza strony nieposiadające certyfikatu SSL jako niebezpieczne. Znacznie zwiększa to prawdopodobieństwo rezygnacji z realizacji zakupów w danym sklepie. - *Świadomość bezpieczeństwa w sieci cały czas rośnie, z większą rozwagą udzielamy też dostępu do naszych danych osobowych, a prywatność stała się istotną wartością. Coraz więcej użytkowników zwraca również uwagę na poziom zabezpieczeń stron. To, czy posiadają one komplet zabezpieczeń można w łatwy sposób sprawdzić przy pomocy specjalnego narzędzia przygotowanego przez nazwa.pl: szybkość i bezpieczeństwo* – tłumaczy Krzysztof Cebrat, prezes zarządu nazwa.pl.

Duet, który zapewnia maksymalną ochronę

Certyfikat SSL (Secure Sockets Layer) oraz protokół sieciowy TLS (Transport Layer Security) stanowią sposób na zabezpieczenie przesyłanych danych. Obecnie na polskim rynku dostępna jest już najnowsza wersja TLS 1.3, która jest wspierana m.in. przez przeglądarki Chrome i Firefox, a po stronie serwerów hostingowych przez firmę nazwa.pl. Wdrożenie przez polskiego lidera branży usług hostingowych protokołu TLS 1.3 przyczyniło się do znacznego wzrostu poziomu bezpieczeństwa serwisów dla setek tysięcy polskich właścicieli stron WWW oraz ich odbiorców. Ważną informacją dla użytkowników dokonujących płatności online jest fakt, że TLS 1.3 jest wspierany przez najnowszą wersję PCI Compliance v3.1 czyli standardu, który zapewnia najwyższy i spójny poziom bezpieczeństwa w środowiskach związanych z przetwarzaniem danych posiadaczy kart płatniczych.

Czym jest certyfikat SSL?

Certyfikat SSL jest narzędziem zapewniającym ochronę pomiędzy przeglądarką internetową a serwerem WWW. Umożliwia on również aktywację protokołu HTTP/2, który przyspiesza komunikację, a co za tym idzie strony WWW znacznie szybciej się wyświetlają. Warto przypomnieć, że w przypadku ładowania się strony dłużej niż 3 sekundy współczynnik odrzuceń rośnie o 100%, dlatego połączenie certyfikatu SSL i HTTP/2 jest tak ważne dla właściciela serwisu. Certyfikaty SSL dzielą się na 3 klasy, które różnią się między sobą poziomem weryfikacji wnioskującego podmiotu. Wyróżniamy certyfikaty: DV (Domain Validation), OV (Organization Validation), EV (Extended Validation). Stopniuje się je według ilości informacji niezbędnych do uzyskania danego poziomu certyfikacji. – *Certyfikat SSL jest najbardziej rozpowszechnionym rozwiązaniem wspierającym bezpieczeństwo transmisji danych w Internecie. W codziennej komunikacji używamy protokołu TLS, który jest rozwinięciem protokołu SSL. Protokół sieciowy TLS stanowi część szyfrowanej wersji HTTPS, jednak jego działanie jest znacznie szerze.* – tłumaczy Rafał Lorenc, dyrektor IT w nazwa.pl.

Dlaczego warto stosować certyfikaty?

Klienci, mając do wyboru dwa sklepy, najprawdopodobniej chętniej zrobią zakupy w tym, który gwarantuje bezpieczeństwo ich danych. Co więcej, Google automatycznie wyżej pozycjonuje strony wyposażone w certyfikaty SSL oraz TLS. Statystyki wskazują też, że 46% stron internetowych w sektorze finansowym i 36% w branży e-commerce, które znajdują się w pierwszej 10 wyników Google w Stanach Zjednoczonych, korzysta z bezpiecznego połączenia HTTPS opatrzonego jednym z certyfikatów. Dlatego szyfrowanie treści staje się koniecznością, a wszelkie incydenty związane z wyciekiem danych klientów stanowią poważną szkodę wizerunkową, która może w widoczny sposób przekładać się na straty finansowe.