Warszawa, 05.02.2019r.

Bezpieczeństwo transakcji internetowych – jak zabezpieczyć przepływ danych w sieci?

Cyberprzestępcy korzystają z coraz bardziej zaawansowanych i wyrafinowanych sposobów wykradania danych osobowych osób poruszających się w Internecie. Na niebezpieczeństwo są również narażone firmy, które oferują możliwość zakupu usług lub produktów online. Jakie zatem zabezpieczenia powinien posiadać e-sklep, aby dokonywanie transakcji było bezpieczne dla klientów?

W dobie licznych i kierunkowych ataków hackerskich, szczegółowe informacje dotyczące zasobów finansowych, ich ulokowania oraz loginów umożliwiających dostęp do kont bankowych są na wagę złota. Trzeba pamiętać, że ich zabezpieczanie leży zarówno po stronie użytkowników, jak i instytucji administrujących tymi danymi. Z tego względu firma, która posiada najnowsze zabezpieczenia ma szansę budować pozytywny wizerunek wśród klientów, chroniąc ich przed kradzieżą poufnych informacji podczas realizacji zamówienia. Można nazwać to podwójną korzyścią, ponieważ sklep jednocześnie buduje wiarygodną markę i zabezpiecza swoich klientów. Pierwszą kwestią, na którą należy zwrócić uwagę, jest etap przepływu danych i ich odpowiednie zabezpieczenie. Podstawowymi narzędziami do zabezpieczenia witryny WWW, które warto poznać, są trzy rozwiązania : DNSSEC, SSL, oraz DNS over TLS.

DNSSEC

Protokołem, który chroni użytkowników przed phishingiem jest DNSSEC. Jest to metoda oszustwa, polegająca na tym, że cyberprzestępca podszywa się pod osobę lub firmę w celu wyłudzenia wrażliwych danych personalnych. Mogą to być na przykład hasła do logowania na stronach bankowych lub dane potrzebne do realizacji płatności. Uzyskuje się je poprzez przekierowanie użytkowników na fikcyjne strony WWW, do złudzenia przypominające te prawdziwe, będące pod tym samym adresem, co właściwa strona. Klienci dokonujący transakcji online są narażeni nie tylko na utratę danych personalnych, ale także na poważne straty finansowe. DNSSEC ma za zadanie nie dopuścić do wyświetlenia innej strony WWW pod daną domeną. Na polskim rynku liderem tej technologii jest nazwa.pl, która zabezpiecza 91% wszystkich domen chronionych tym protokołem.

SSL – podstawa w szyfrowaniu danych

SSL jest protokołem sieciowym szyfrującym informacje, zapewniającym poufność transmisji danych przesyłanych pomiędzy osobą odwiedzającą stronę WWW a fizycznym serwerem, na którym się znajdują. Dodatkowym zabezpieczeniem stosowanym przy implementacji SSL jest protokół CAA. Poprzez to rozwiązanie właściciel domeny określa, który Urząd Certyfikacji może wystawić dla danej domeny certyfikat szyfrujący. Szyfrowanie jest oznaczone skrótem HTTPS (Hypertext Transfer Protocol Secure), wyświetlanym na początku adresu strony. Oznacza to, że podczas przeglądania witryny WWW najpierw następuje wymiana kluczy kryptograficznych, a dopiero potem standardowe żądanie o przesłanie strony WWW. Jak rozpoznać czy dany adres WWW wykorzystuje protokół SSL? Witryna prawidłowo zabezpieczona certyfikatem jest łatwa do odróżnienia – po lewej stronie adresu strony w przeglądarce widnieje symbol zielonej kłódki. Co więcej, obecnie przeglądarka Google Chrome automatycznie oznacza strony bez tego certyfikatu jako potencjalnie niebezpieczne.

DNS over TLS

DNS over TLS w skrócie jest ochroną przed inwigilacją zapytań do DNS, zapewniającą użytkownikowi prywatność w zakresie wyszukiwanych stron czy adresów. DNS działa jak książka telefoniczna, która zamienia nazwy domen na adresy IP. Przed otwarciem strony WWW lub wysłaniem wiadomości e-mail konieczne jest ustalenie adresu IP serwera w sieci. W tym celu komputer łączy się z serwerem DNS, obsługującym daną domenę i ustala dokładny adres IP. Zwykłe zapytanie jest przekazywane otwartym tekstem, umożliwiającym podsłuchanie transmisji i dokładne ustalenie, z jakiej strony WWW korzysta użytkownik. DNS over TLS funkcjonuje na podobnej zasadzie, jak ma to miejsce w przypadku szyfrowania transmisji stron WWW zabezpieczonych przy użyciu certyfikatów SSL, chroniąc przesyłane dane przed podsłuchaniem przez osoby nie uprawnione. W tym miejscu warto jednak wyjaśnić, że DNS over TLS chroni prywatność przesyłanych zapytań i odpowiedzi z systemu DNS, natomiast weryfikacją poprawności przesyłanych danych zajmuje się inne zabezpieczenie, czyli wcześniej wspomniany DNSSEC.

Bezpieczeństwo buduje zaufanie

Warto uświadamiać swoim klientom zagrożenia płynące z nieodpowiedzialnego korzystania z Internetu, a także to, że raz nieopatrznie udostępnione dane w sieci mogą w niej zostać na długo. Należy również podkreślać, jak ważne jest bezpieczeństwo podczas dokonywania transakcji online. Decydując się na szereg rozwiązań z zakresu bezpieczeństwa, zapewniamy klientom komfort poruszania się po witrynie oraz ciągłość jej działania. Wpływa to zarówno na budowanie grona zadowolonych klientów, jak i przyczynia się do rozwoju biznesu. Kompleksową ochronę zapewnia pakiet Bezpieczna Domena w nazwa.pl, dzięki któremu właściciel witryny posiada najlepiej zabezpieczoną domenę w Polsce.