CertyfikatySSL.pl

PREZENTUJĄ

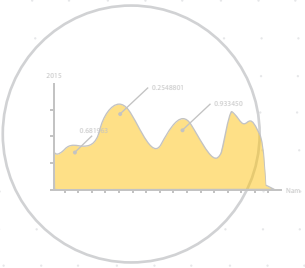
PORADNIK SSL I SEO

KOMPLETNY PRZEWODNIK PO SSL I SEO

Google ogłosił, że obecność protokołu HTTPS jest jednym z czynników branych pod uwagę w algorytmie wyszukiwarki i ma coraz większe znaczenie w rankingu pozycji strony. Zgodnie z zapowiedzią Google, opublikowaną 6 sierpnia 2014 na blogu Google, strony z HTTPS, stosujące certyfikat SSL z 2048-bitowym kluczem, otrzymują dodatkowy impuls i szybciej pną się w wynikach wyszukiwarki. Obecnie ich wpływ jest jeszcze minimalny, ale Google zapowiada wzrost znaczenia HTTPS na pozycje stron w najbliższym czasie.

Co to jest SSL?
SSL (z ang. Secure Sockets Layer) to protokół, który szyfruje połączenia między stroną internetową a użytkownikiem. SSL chroni prywatność użytkownika, a także zabezpiecza witrynę i usługi przed niektórymi atakami. Co więcej certyfikaty SSL uwiarygodniają stronę www. Gdy użytkownik widzi, że strona posiada certyfikat wie, że jest ona prawdziwa i zarządzana przez prawidłowy podmiot. Google dąży do tego, aby zapewnić swoim użytkownikom bezpieczne i wiarygodne przeglądanie Internetu. Nic więc dziwnego, że zdecydowało się na wdrożenie protokołu HTTPS jako czynnika wpływającego na wyniki wyszukiwania.

Webmasterzy, którzy chcą skorzystać z możliwości zwiększenia pozycji w wyszukiwarce, a jednocześnie zależy im na zapewnieniu prywatności i bezpieczeństwa swoim użytkownikom, powinni przenieść swoje strony z HTTP na HTTPS. Proces zmiany strony różni się w zależności od środowiska i potrzeb witryny. Aby Google zanotowało zmiany przede wszystkim niezbędna jest prawidłowa konfiguracja serwera, każdy element na stronie musi być zastosowany przy użyciu protokołu HTTPS (Always On SSL) oraz dodatkowo optymalizacja innych czynników. Zmiany są konieczne. Google przyznał, że pracuje nad tym, aby Internet był bardziej bezpieczny, dlatego promuje wyniki pochodzące z wiarygodnych witryn zawierających wysoką jakość informacji. Google chce mieć pewność, że strony które odwiedzają jego użytkownicy są bezpieczne. Obecnie wpływ HTTPS na pozycje strony w wyszukiwarce jest niewielki, ale będzie sukcesywnie zwiększał się w czasie.



KROK 1
WYBÓR ODPOWIEDNIEGO CERTYFIKATU SSL DLA WITRYNY INTERNETOWEJ

Rodzaje walidacji

Istnieją trzy klasy walidacji do wyboru: DV (ang. Domain Validation, pol. walidacja domeny), OV (ang. Organization Validation, pol. walidacja organizacji/firmy) oraz EV (ang. Extended Validation, pol. rozszerzona walidacja). Aby zastosować certyfikat do strony internetowej należy spełnić odpowiednie warunki w zależności od wybranej walidacji.

Walidacja DV wymaga od nabywcy jedynie świadectwa posiadania dostępu do konta e-mail administratora witryny, czyli możliwości zidentyfikowania posiadacza certyfikatu DV jako właściciela-operatora domeny.

Walidacja OV wymaga sprawdzenia nie tylko domeny, ale również firmy. Do skorzystania z walidacji OV organizacja musi wykazać, że prowadzona działalność gospodarcza jest działalnością legalną. Dodatkowy poziom weryfikacji jest stosowany, ponieważ OV ustanawia wyższy poziom zaufania użytkowników do danej witryny. Jest on stosowany dla wszystkich przedsiębiorstw bez względu na ich wielkość.

Walidacja EV wymaga tego samego procesu weryfikacji jak OV. Ponadto certyfikat EV dodaje wizualnego znaku witrynie w pasku adresowym przeglądarki internetowej. Strony z certyfikatami EV mają podświetloną na zielono nazwę firmy, która pojawia się bezpośrednio przed adresem www.
Certyfikaty EV są powszechnie stosowane przez duże firmy, tak aby użytkownicy ich stron internetowych byli natychmiast po wejściu na stronę zapewniani, że ich prywatność i dane są zabezpieczone.

W zapowiedzi Google I / O 2014 – „HTTPS everywhere", Ilya Grogorik i Pierre Far podkreślili znaczenie HTTPS nie tylko dla szyfrowania SSL, ale również dla zapewnienia wiarygodności strony. Przeprowadzone badania wykazały znacznie wyższy współczynnik konwersji ze stron, które używały certyfikatów OV, a jeszcze wyższy przy użyciu certyfikatów EV. Jest to spowodowane zaufaniem odwiedzających do stron dbających o bezpieczeństwo. Google rekomenduje strony potwierdzające swoją wiarygodność certyfikatem SSL, OV i EV, dlatego też warto zastosować jeden z nich przy swojej stronie, jeśli tylko wymaga ona od użytkownika zostawiania danych prywatnych.

Rodzaje certyfikatów

Po wybraniu najlepszej dla swojej strony www walidacji należy ocenić potrzeby witryny oraz wybrać jeden z trzech rodzajów certyfikatów: Certyfikaty SSL Single Domain, Certyfikaty SSL Wildcard lub Certyfikaty SSL Multi-Domain.

Certyfikaty SSL Single Domain są przeznaczone dla właściciela jednej strony internetowej, która nie posiada subdomeny.

Certyfikaty SSL Wildcard służą do szyfrowania głównej domeny (np. certyfikatyssl.pl) oraz nieograniczonej ilości jej subdomen pierwszego poziomu (np. mail.certyfikatyssl.pl, sklep.certyfikatyssl.pl, smtp.certyfikatyssl.pl).

Certyfikaty SSL Multi-Domain są przeznaczone dla podmiotów zarządzających wieloma stronami internetowymi w ramach jednej organizacji. Na przykład Jnj.com posiada również domeny Tylenlol.com, Neutrogena.com i Rembrandt.com. SSL Multi-Domain sprawia, że zarządzanie certyfikatami SSL dla wszystkich domen jest znacznie łatwiejsze i bardziej korzystne finansowo niż użycie certyfikatów SSL Single Domain dla każdej domeny indywidualnie.

Uwaga: Niezależnie od tego, który typ certyfikatu SSL wybierzesz, pamiętaj o wydaniu certyfikatu za pomocą SHA-256, a nie SHA-1. Wiele wyszukiwarek, w tym Google, kładzie nacisk na stosowanie SHA-256. Ponadto certyfikaty wydawane za pomocą SHA-1 będą uznawane jedynie do końca 2014 roku.

KROK 2
AKTUALIZACJA I WERYFIKACJA INFORMACJI O FIRMIE

Przed zakupem certyfikatu SSL i generowaniem pliku CSR wszystkie dane w bazie WHOIS muszą być aktualne, a firma musi być prawidłowo wyświetlana w niezależnych katalogach i bazach.

Weryfikacja danych WHOIS

Aby sprawdzić dokładność danych WHOIS, należy przejść do http://domeny.pl/whois.html, wpisać adres domeny i wybrać „Sprawdź". Jeśli dane są nieprawidłowe, należy zalogować się do panelu kontrolnego i dokonać odpowiednich aktualizacji / zmian w koncie.

Uwaga: Ochrona prywatności WHOIS w przypadku domen globalnych musi być wyłączona w trakcie procesu. Ochrona prywatności może zostać przywrócona po otrzymaniu certyfikatu SSL.

Weryfikacja dopasowania danych w bazach

Urząd Certyfikacyjny przed wydaniem certyfikatu SSL sprawdza, czy dane w bazie WHOIS odpowiadają informacjom zawartym w oficjalnych bazach. Często Urzędy Certyfikacji przeprowadzają weryfikację danych przy użyciu stron państwowych np. ems.ms.gov.pl. Ważne jest, aby numer telefonu znajdujący się na liście był aktualny, gdyż jest on używany przez Urząd Certyfikacji przy weryfikacji telefonicznej.

Weryfikacja DCV

Do wykonania konfiguracji należy posiadać dostęp do adresu e-mail, który zostanie użyty do odbioru wiadomości Domain Control Validation (DCV). Dopuszczalne e-maile do weryfikacji to: admin@, administrator@, webmaster@, hostmaster@ bądź e-mail zarejestrowany w bazie WHOIS.

Weryfikacja SNI / dedykowanego adresu IP

Przed dokonaniem zakupu i instalacji certyfikatu SSL należy sprawdzić i upewnić się, że jest się w posiadaniu SNI bądź dedykowanego adresu IP. Bez włączonego dedykowanego adresu IP lub SNI instalacja certyfikatu SSL nie będzie możliwa.

KROK 3
ZAKUP CERTYFIKATU SSL I GENEROWANIE CSR

Następnym krokiem po wybraniu właściwej walidacji, dokonaniu weryfikacji danych WHOIS i zakupie certyfikatu jest wygenerowanie żądania wydania certyfikatu (CSR ang. Certificate Signing Request). Podczas generowania pliku CSR ważne jest, aby wprowadzone dane były identyczne jak podane w bazie WHOIS.

Podczas generowania pliku CSR, tworzony jest również prywatny klucz (Private Key). Należy zapisać klucz w bezpiecznym miejscu. Należy pamiętać, że każdy, kto otrzyma dostęp do prywatnego klucza, będzie miał dostęp do zaszyfrowanych informacji.

Podczas generowania pliku CSR należy wypełnić formularz kontaktowy i podać adres e-mail, który będzie używany do weryfikacji DCV. Gdy plik CSR zostanie wygenerowany, a formularz wypełniony, wniosek zostanie wysłany do urzędu certyfikacji, który skontaktuje się w celu zakończenia procesu weryfikacyjnego i wydania certyfikatu.
Uwaga: Aby ułatwić i przyspieszyć wydanie certyfikatu niektóre Urzędy Certyfikacji mogą prosić o podanie numeru DUNS.

Uwaga: dla Certyfikatu SSL Wildcard - podczas generowania pliku CSR używanego do certyfikatu SSL Wildcard, pamiętaj o dodaniu gwiazdki przed nazwą domeny (np. *.certyfikatyssl.pl). To zagwarantuje poprawną konfigurację certyfikatu SSL dla wszystkich subdomen.

Aby zobaczyć, jak działa narzędzie do generowania pliku CSR, zachęcamy do skorzystania z bezpłatnego generatora pliku CSR.

KROK 4
INSTALACJA CERTYFIKATU SSL ORAZ OPTYMALIZACJA WITRYNY

Przed zainstalowaniem certyfikatu, zaleca się, aby serwer działał na najnowszej wersji systemu operacyjnego (OS). Po dokonaniu wcześniejszych działań nadszedł czas na zainstalowanie certyfikatu SSL. Dla większości serwerów / paneli kontrolnych instalacja certyfikatu jest bardzo prosta: kopiuj i wklej certyfikat do panelu w postaci zwykłego tekstu.

Uwaga: Rekomendowane jest stosowanie systemu operacyjnego, który jest kompatybilny z minimalnymi wymaganiami protokołów bezpieczeństwa i szyfrowania.

Pełny wykaz protokołów instalacji znajdziesz na w Bazie Wiedzy serwisu CertyfikatySSL.pl.

Po zakończeniu instalacji certyfikatu SSL (skopiuj i wklej) użytkownik otrzyma możliwość dostępu do strony zarówno przez HTTPS, jak i HTTPS. Pod kątem SEO, posiadanie obu adresów jest uznawane jako „duplikaty strony" (duplicate content).
Pod kątem bezpieczeństwa strona nadal jest narażona na zagrożenie. Pierwszym krokiem do rozwiązania tego problemu jest przekierowanie całego ruchu z HTTP na HTTPS. Można to zrobić w ustawieniach serwera lub poprzez edycję reguł umieszczonych w pliku .htaccess (Apache) w folderze publicznym html.

Przykład

Serwer Apache domyślnie zezwala na połączenie TLS, ale będzie mógł użyć pliku .htaccess tylko wtedy, gdy plik konfiguracji Apache (httpd.conf lub conf.d/ lub sites-enabled/) zezwala na podążanie za łączem symbolicznym.

```
RewriteEngine ON
RewriteCond %{HTTP_HOST} ^adres.pl$
RewriteRule ^(.*) https://www.example.com/$1 [QSA,L,R=301]
```

Uwaga: Aktualne informacje na temat konfiguracji serwera znajdziesz na stronie Mozilla's recommend configurations.

Jeśli witryna stosuje CMS należy wykonać kilka kroków, aby włączyć protokół SSL. Dla przykładu, jeśli strona posiada WordPress, należy wybrać kolejno następujące funkcje Panel Administratora -> Ustawienia -> Ogólne i upewnić się, że zarówno adres WordPress (URL) i adres strony (URL) są skonfigurowane do protokołu HTTPS. Jeśli nie, należy po prostu dodać "s" po HTTP i zapisać zmiany.

KROK 5
OPTYMALIZACJA SERWERA

Optymalizacja serwera zwiększa ogólne bezpieczeństwo witryny, rozwiązuje wszelkie problemy i sprawia, że strona działa efektywniej. Należy pamiętać, że bez Root Access dostęp do części lub wszystkich protokołów może być utrudniony.

HTTP Strict Transport Security (HSTS) przyspiesza SSL informując przeglądarkę, aby zawsze łączyła się przy użyciu protokołu HTTPS i automatycznie przełączała żądania z HTTP na HTTPS, unikając dzięki temu angażowania serwera w tym celu.

SPDY (Pronounced Speedy) to moduł opracowany przez Google w celu przyspieszenia połączeń TLS przez multipleksowanie wielu zapytań za pośrednictwem jednego połączenia. Niestety, to użyteczne narzędzie nie jest kompatybilne ze wszystkimi serwerami. Należy sprawdzić czy SPDY będzie działać dla konkretnego serwera – można to zrobić na stronie http://spdycheck.org/.

Online Certificate Status Protocol (OCSP) służy do sprawdzania, czy certyfikat został unieważniony. Przeglądarka sprawdza tą informację, ale stosując OCSP serwer jest w stanie wysłać certyfikat i przedstawić informacje z wniosku o wydanie certyfikatu. Dzięki temu przeglądarka nie musi pobierać informacji z Urzędu Certyfikacji.

HTTPS Keep Alives utrzymuje otwarte połączenie, eliminując fazę „handshake" przy kolejnych połączeniach pomiędzy przeglądarką a serwerem. Jest to szczególnie ważne, jeśli użytkownikowi zależy na szybkim działaniu strony. Połączenia TCP rozpoczynają powoli i zwiększają swoją prędkość, aż do osiągnięcia maksymalnych możliwości. Aby zwiększyć prędkość połączeń należy dać użytkownikowi wystarczający czas na wykonanie kolejnego kroku zanim połączenie się zakończy. Optymalnym czasem na początek jest 60 sekund. Zdarza się, że ustawienia przeglądarki użytkownika mogą być nadrzędne w stosunku do Keep Alives. Dlatego też, należy zapoznać się w pełni z możliwościami Keep Alives i wybrać najlepsze rozwiązanie dla swojej witryny.

Wznowienie sesji i cookies pozwalają serwerom i przeglądarkom na szybszą komunikację poprzez zmniejszanie czasu potrzebnego na nawiązanie połączenia (handshake). Odwiedzając stronę przeglądarka zapisuje plik tzw. cookies. Po powrocie na witrynę cookies informuje, że szyfrowanie było już wcześniej negocjowane i powinno być wznowione. Metoda ta powinna być używana z rozwagą, gdyż cookies są równie istotne, jak klucz prywatny.

KROK 6
TESTOWANIE STRONY INTERNETOWEJ I KONFIGURACJA SERWERA

Ostatnim krokiem w migracji HTTPS jest przetestowanie serwera / strony internetowej, aby mieć pewność, że protokoły są aktualne oraz że strona jest poprawnie skonfigurowana i działa prawidłowo.

Test serwera i certyfikatu

Test serwera pozwoli ocenić stopień jego zabezpieczenia oraz poda informacje, jakich zmian można dokonać w celu zwiększenia bezpieczeństwa posiadanego serwisu. Należy pamiętać, że zwiększona ilość zabezpieczeń może ograniczyć dostęp do witryny niektórym klientom (korzystającym ze starszych przeglądarek). Narzędzia do testowania dostępne są tu: https://certyfikatyssl.pl/ssl-tools.html.

Skanowanie zmieszanej treści

Jeżeli istnieje jakakolwiek mieszana zawartość na witrynie (strona, która obejmuje zarówno HTTP i HTTPS), należy zmienić treść HTTP na linki względne lub zakodować je na sztywno z HTTPS. Zaleca się używanie linkowania względnego, ponieważ znacznie łatwiej jest przenieść stronę pomiędzy środowiskiem projektowym a produkcją.

W celu uzyskania wyższych pozycji w wyszukiwarce Google, należy pamiętać, aby nie blokować witryny HTTPS przed indeksowaniem w wyszukiwarce. W tym celu należy zezwolić na indeksowanie stron robotom poprzez plik robots.txt, a następnie monitorować postępy migracji w Webmaster Tools.

KONFIGUROWANIE PRZYCISKÓW SERWISÓW SPOŁECZNOŚCIOWYCH

Po migracji z HTTP na HTTPS statystyki udostępnień na portalach społecznościowych zliczane dla witryny spadną do zera. Powodem tego jest fakt, że serwisy te odczytują http://www.twojadomena.com jako inny adres URL niż https://www.twojadomena.com. Istnieje sposób, aby w dalszym ciągu statystyki udostępnień się zgadzały. Wystarczy napisać odpowiedni kod.

```
<?php
$httpurl = "http://www.".$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF'];
$httpsurl = "https://www.".$_SERVER['HTTP_HOST'].$_SERVER['PHP_SELF'];
 echo "
<div class='fb-like' data-href='".$httpurl."' data-send='false' data-
layout='box_count'></div>

<a href='https://twitter.com/share' class='twitter-share-button' data-
counturl='".$httpurl."' data-url='".$httpsurl."' data-count='vertical' data-
via='moz'>Tweet</a>

<div class='g-plusone' data-size='tall' data-href='".$httpurl."'></div>
";
?>
```

Niestety nie jest to kompletne rozwiązanie. Powyższy kod wyświetli liczbę udostępnień na stronach HTTP, nawet jeśli później zostaną one przeliczone dla HTTPS. Dlatego też podany kod sprawdzi się dla starszych postów. Należy jednak pamiętać, że kolejne udostępnienia nie zostaną dokładnie przeliczone.

Dla nowych postów, wstawionych na portale po zmianie HTTP na HTTPS, podany kod należy zmodyfikować. Dla tych postów należy wskazać liczbę udostępnień na stronach HTTPS, a nie HTTP.
Po wprowadzeniu tych zmian zliczanie udostępnień będzie działać poprawnie na Facebook, Twitter i Google Plus.

PODSTAWOWE ZAGADNIENIA SEO

Wiele kroków związanych z SEO wymaga zmiany HTTP na HTTPS. Oto najważniejsze z nich:

Konfigurowanie przycisków udostępniania na serwisach społecznościowych:

1. Upewnij się, że wszystko na stronie www zostało w przekształcone z HTTP na HTTPS. W przeciwnym wypadku odwiedzający stronę otrzymają komunikaty o błędach certyfikatu bezpieczeństwa. Wszystkie absolutne linki na stronie muszą zostać zmienione z HTTP na HTTPS.

2. Oznacz to również konieczność zmiany w widżetach i pluginach, np. wyszukiwarce na stronie. Należy upewnić się, że odesłania do plików CSS i Javascript oraz wszystkie odnośniki w tych plikach zostały zmienione z HTTP na HTTPS. Podobnie należy zmienić adresu obrazków na stronie.

3. Inne pliki, które również muszą być sprawdzone i zaktualizowane to:

Mapa strony
Robots.txt
plik .htaccess (w przypadku serwerów Apache)

4. Konieczne jest zastosowanie przekierowania 301 z adresu głównego HTTP na HTTPS. Jak radziliśmy już wcześniej, zaleca się zastosowanie HSTS w celu ustalenia HTTPS jako domyślnego adresu dla przeglądarki internetowej (wpływa to pozytywnie na szybkość ładowania strony www), ale mimo to należy ustawić przekierowanie 301 w celu przekazania mocy strony na adres HTTPS.

Należy skonfigurować konto Webmaster Tools dla adresu z HTTPS. Dotychczasowe ustawienia Webmaster Tools dla adresu HTTP nie dostarczą poprawnych danych na temat strony www, gdyż wyszukiwarka odróżnia HTTP od HTTPS i traktuje te adresy jako osobne strony www.

Jeśli przy Twojej stronie www były wykonywane działania mające na celu usuwanie linków historycznych należy sprawdzić i upewnić się, że te linki nie zostaną potraktowane przez Google, jako linki prowadzące do nowej strony HTTPS.

CZĘSTE PROBLEMY

Podczas zmiany strony z HTTP na HTTPS występują typowe problemy. Najczęściej pojawiającymi się są:

1. Content Delivery Networks (CDN) Incompatible (niezgodny) – jeśli użytkownik stosuje CDN w celu przyspieszenia działania witryny internetowej, podczas zmiany z HTTP na HTTPS może wystąpić problem. Większość CDN, w tym Akamai, nie obsługują SSL.
Jednakże Cloudflare obsługuje protokół SSL.

2. Site Search Tools (i inne widżety) generuje błędy bezpieczeństwa – konieczna może być aktualizacja widżetów używanych na stronie.