extranet
internet creator

87-100 Toruń, ul. Wielki Rów 40B, NIP: 879-118-34-25
tel.: +48 61 97 514, +48 665 430 267, fax: +48 61 97 518
e-mail: biuro@extranet.pl, strona internetowa: www.extranet.pl

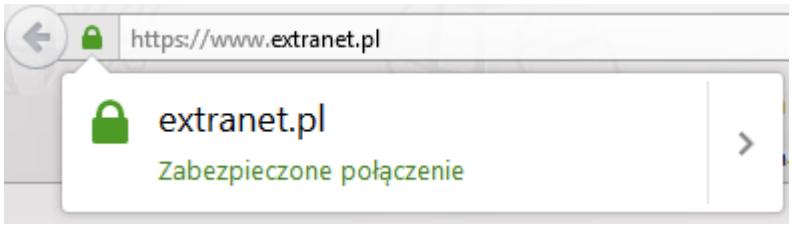
Bezpłatne uzyskanie i wdrożenie darmowego certyfikatu SSL

Wstęp

SSL jest protokołem sieciowym używanym do bezpiecznych połączeń internetowych, który przyjął się jako standard szyfrowania na stronach WWW.

Dzięki projektowi „Let's Encrypt"[1], rozwijanemu przez Internet Security Research Group, firma extranet umożliwia Państwu **bezkosztowe** przeprowadzenie instalacji **darmowego** certyfikatu SSL dla Państwa stron internetowych utrzymywanych na serwerach naszej firmy.

Korzystanie z certyfikatu SSL spowoduje zmianę adresów internetowych Państwa stron internetowych z np. http://www.extranet.pl na https://www.extranet.pl (w części adresu związanego z protokołem do zapisu „http" dochodzi litera "s") wraz z wyświetlaniem się w pasku adresu przeglądarki internetowej charakterystycznego znaku kłódki.



Czy certyfikat SSL jest potrzebny?

Przeglądarki internetowe, począwszy od Google Chrome w wersji 62 (październik 2017), zaczynają wprowadzanie dodatkowych oznaczeń w pasku adresu stron internetowych nie posiadających certyfikatu SSL - pierwszym etapem jest oznaczanie wybranych podstron etykietą „**Niebezpieczna**" (z ang. „Not secure"), a następnie wszystkich stron internetowych nie posiadających certyfikatu SSL.

Już teraz warto zadać pytanie czy internauci odwiedzający Twoją stronę internetową będą nadal to robić widząc etykietę „**Niebezpieczna**".

1 https://letsencrypt.org

87-100 Toruń, ul. Wielki Rów 40B, NIP: 879-118-34-25
tel.: +48 61 97 514, +48 665 430 267, fax: +48 61 97 518
e-mail: biuro@extranet.pl, strona internetowa: www.extranet.pl

Czy certyfikat SSL jest obowiązkowy?

Dla stron internetowych, których funkcjonalność umożliwia przesyłanie danych wykorzystywanych do uwierzytelnienia (np. logowanie do intranetu, dostęp do panelu administracyjnego), posiadanie zabezpieczeń kryptograficznych jest **wymagane** przez polskie prawo[2].

Dodatkowo 9 czerwca 2017 r. Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Unii Europejskiej przedstawiła projekt regulacji zakładających m. in. wymuszenie stosowania metod kryptograficznych (np. certyfikaty SSL dla stron internetowych) wszędzie tam, gdzie jest to technicznie możliwe[3] co stanowi sygnał, że w niedalekiej przyszłości regulacja stanie się wymogiem prawa unijnego.

Jakie korzyści daje certyfikat SSL?

Główne korzyści wprowadzenia certyfikatu SSL:

- poczucie bezpieczeństwa internautów - informacje przesyłane pomiędzy przeglądarką internetową użytkownika a serwerem, na którym znajduje się strona internetowa są szyfrowane, co jest ważne szczególnie w przypadku przesyłania poufnych informacji (np. danych osobowych);
- wiarygodność instytucji - certyfikat SSL potwierdza wiarygodność strony WWW, a w przypadku wykorzystywania bardziej zaawansowanych certyfikatów typu EV, oferowanych przez firmy komercyjne, również wiarygodność całej instytucji;
- lepsze pozycjonowanie strony WWW - korzystanie z certyfikatu SSL może powodować wzrost pozycji strony WWW w wynikach wyszukiwarek internetowych (np. Google)[4];
- szybsze działanie strony WWW - prędkość ładowania stron internetowych zwiększa się dzięki protokołom SPDY[5] czy HTTP/2[6] obsługiwanych przez nowoczesne przeglądarki internetowe.

2 rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – załącznik rozdział C. XIII (Dz. U. z 2004 r. Nr 100, poz. 1024 - http://dziennikustaw.gov.pl/DU/2004/1024/1) będący aktem wykonawczym do ustawy o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 - http://dziennikustaw.gov.pl/DU/2016/922/1)

3 „Eurodeputowani opowiedzieli się za szyfrowaniem komunikacji dla wszystkich obywateli UE" - http://antyweb.pl/szyfrowanie-komunikacji-dla-wszystkich-obywateli-ue; dokument źródłowy: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-606.011%2B01%2BDOC%2BPDF%2BV0%2F%2FEN (Amendment 116 na stronie 74)

4 artykuł "HTTPS as a ranking signal"; http://googlewebmastercentral.blogspot.com/2014/08/https-as-ranking-signal.html [z dnia 2014.08.06 w języku angielskim]

5 artykuł "SPDY"; https://pl.wikipedia.org/wiki/SPDY

6 https://en.wikipedia.org/wiki/HTTP/2

87-100 Toruń, ul. Wielki Rów 40B, NIP: 879-118-34-25
tel.: +48 61 97 514, +48 665 430 267, fax: +48 61 97 518
e-mail: biuro@extranet.pl, strona internetowa: www.extranet.pl

Czy mogą wystąpić problemy?

Konsekwencją wprowadzenia certyfikatu SSL dla strony internetowe będzie brak możliwości korzystania ze stron internetowych przy wykorzystywaniu archaicznych przeglądarek internetowych[7]; sytuacja jest niszowa[8] i dotyczy przede wszystkim użytkowników przeglądarki internetowej Microsoft Internet Explorer działających pod kontrolą niewspieranego już od kwietnia 2014 r. systemu operacyjnego Microsoft Windows XP - rozwiązaniem tego problemu jest zainstalowanie i korzystanie z nowoczesnej, w pełni darmowej przeglądarki internetowej Mozilla Firefox[9] (niestety rozwiązanie nie dotyczy przeglądarek Google Chrome[10] i Opera[11]).

Co zrobić, aby posiadać certyfikat SSL na stronie WWW?

Wystarczy przesłanie prośby o instalację certyfikatu SSL w wiadomości e-mail na adres admin@extranet.pl o tytule "Darmowy certyfikat SSL".

Otrzymają Państwo informację zwrotną o przeprowadzonej operacji.

Czy operacja jest odwracalna?

W celu usunięcia certyfikatu SSL ze strony WWW wystarczy przesłanie prośby o usunięcie certyfikatu SSL w wiadomości e-mail na adres admin@extranet.pl o tytule „Usunięcie certyfikatu SSL”.

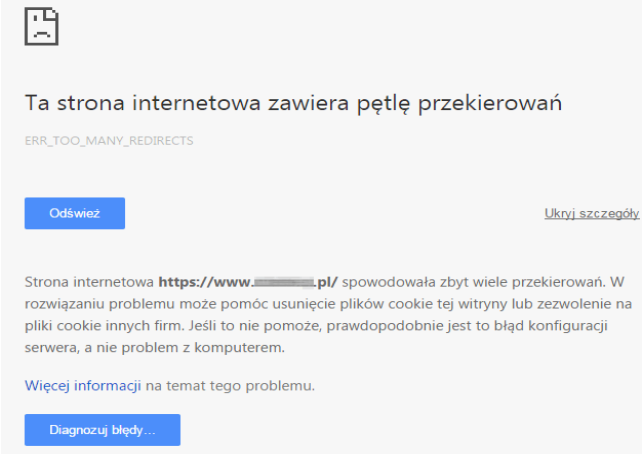
Konsekwencjami rezygnacji z certyfikatu SSL są:

1. zmiana adresu strony internetowej (powrót do zapisu protokołu „http” bez litery „s” na końcu) i nie wyświetlanie się już w pasku adresu przeglądarki internetowej charakterystycznego znaku kłódki,
2. internauci, którzy już odwiedzali stronę internetową, będą musieli wyczyścić pamięć podręczną przeglądarki internetowej, ponieważ będą one „pamiętać” informację o konieczności prowadzenia bezpiecznej szyfrowanej komunikacji (po pewnym czasie

7 https://en.wikipedia.org/wiki/Server_Name_Indication#No_support
8 w Polsce niecałe 6% zapytań HTTPS; https://blog.cloudflare.com/introducing-universal-ssl/ [z dnia 2014.08.29 w języku angielskim]
9 https://support.mozilla.org/en-US/kb/end-support-windows-xp-and-vista [w języku angielskim]
10 https://chrome.googleblog.com/2015/11/updates-to-chrome-platform-support.html [z dnia 2015.11.10 w języku angielskim]
11 https://blogs.opera.com/news/2016/04/chrome-alternative-opera-for-windows-xp-vista/ [z dnia 2016.04.15 w języku angielskim]

87-100 Toruń, ul. Wielki Rów 40B, NIP: 879-118-34-25
tel.: +48 61 97 514, +48 665 430 267, fax: +48 61 97 518
e-mail: biuro@extranet.pl, strona internetowa: www.extranet.pl

przeglądarki samodzielnie usuwają takie informacje).



Przykładowy komunikat przeglądarki

Gdzie mogę znaleźć więcej informacji?

Poniżej prezentujemy wybrane artykuły związane z certyfikatami SSL:

- „Zabezpiecz swoją witrynę za pomocą protokołu HTTPS”:

  https://support.google.com/webmasters/answer/6073543?hl=pl
- „Avoiding the Not Secure Warning in Chrome” (w języku angielskim):

  https://developers.google.com/web/updates/2016/10/avoid-not-secure-warn [z października 2016]
- „Twórcy Chrome chcą ostrzegać przed witrynami, które nie używają HTTPS”:

  https://www.dobreprogramy.pl/Tworcy-Chrome-chca-ostrzegac-przed-witrynami-ktore-nie-uzywaja-HTTPS,News,59856.html [z dnia 2014.12.16]
- „Dzięki Let's Encrypt szyfrowanie stron będzie łatwiejsze i darmowe”

  https://www.dobreprogramy.pl/Dzieki-Lets-Encrypt-szyfrowanie-stron-bedzie-latwiejsze-i-darmowe,News,59266.html [z dnia 2014.11.19]
- „Google promuje strony HTTPS - kto musi kupić certyfikat? ”

  https://tech.wp.pl/kat,1009785,title,Google-promuje-strony-HTTPS-kto-musi-kupic-certyfikat,wid,16822162,wiadomosc.html [z dnia 2014-08-18]
- „Google będzie lepiej pozycjonował strony wykorzystujące protokół HTTPS”:

  http://antyweb.pl/google-bedzie-lepiej-pozycjonowal-strony-wykorzystujace-protokol-https/ [z dnia 2014.08.07]
- „Pozycjonowanie przez Google stron opartych na HTTPS”:

87-100 Toruń, ul. Wielki Rów 40B, NIP: 879-118-34-25
tel.: +48 61 97 514, +48 665 430 267, fax: +48 61 97 518
e-mail: biuro@extranet.pl, strona internetowa: www.extranet.pl

http://nf.pl/manager/konsekwencje-promowania-przez-google-stron-opartych-na-https,,48863,60 [z dnia 2014.08.19]