***Protokół HTTPS***

1. **Definicja protokołu HTTPS**.

HTTPS - czyli Hypertext Transfer Protocol Secure, to protokół komunikacyjny wykorzystywany w Internecie do bezpiecznej transmisji danych. Jest to bezpieczna wersja protokołu HTTP, gdzie dodano warstwę SSL/TLS w celu zaszyfrowania danych przesyłanych między klientem a serwerem.

1. **Różnica między protokołem HTTP a HTTPS**

HTTP i HTTPS to dwa protokoły używane do przesyłania danych w Internecie, ale różnią się głównie pod względem bezpieczeństwa.

|  |  |
| --- | --- |
| HTTP | HTTPS |
| Przesyła dane w formie niezaszyfrowanej. | Przesyła dane w formie zaszyfrowanej |
| Nie wymaga certyfikatów SSL/TLS. | Używa protokołów kryptograficznych (SSL/TLS) do zaszyfrowania danych. |
| Działa na standardowym porcie 80. | Działa na standardowym porcie 443. |
| Jest podatny na przechwycenie danych przez osoby trzecie. |  |

1. **Jak działa HTTPS**

Na początkuuzgadniana jest tożsamość serwera oraz urządzenia użytkownika. Kolejnym krokiem jest wymiana wiadomości zawierających informacje, które umożliwią później nawiązanie interakcji pomiędzy stronami. Po zakończeniu tej interakcji, dochodzi do wymiany certyfikatów i gdy wszystko jest w porządku, przekazywane są klucze szyfrujące. Dzięki nim możliwe jest przesyłanie zaszyfrowanych danych i ich poprawne odbieranie przez uczestników komunikacji, czyli przez serwer i urządzenie odbierające, z którego korzysta użytkownik. Jednocześnie szyfrowanie sprawia, że nawet przechwycone przez niepowołane osoby dane nie zostaną odtworzone i nie dojdzie do utracenia poufnych danych.

1. **Rodzaje certyfikatów SSL/TLS**

Istnieją trzy podstawowe typy certyfikatów SSL, które określa się na podstawie poziomu weryfikacji (walidacji) danego podmiotu, jakiemu wydaje się certyfikat.

1. **Certyfikat DV (Domain Validation)** – czyli certyfikat z weryfikacją domeny. Walidacja dokonuje się w sposób zautomatyzowany i obejmuje informacje zgromadzone w systemie DNS dla domeny danego serwera oraz dane podmiotu ubiegającego się o certyfikat. Weryfikacja nie obejmuje natomiast danych organizacji. W certyfikacie DV zawarta jest jedynie nazwa domeny bez żadnych dodatkowych informacji o podmiocie.  
     
   Certyfikat DV jest najtańszy, a jego wystawienie trwa zaledwie parę minut. Zautomatyzowanie całego procesu wiąże się jednak z pewnymi ograniczeniami. Certyfikaty te potwierdzają bezpieczeństwo danej strony, ale nie dostarczają żadnej wiedzy o jej wydawcy. Dlatego sprawdzają się w przypadku takich transmisji danych, które odbywają się między ufającymi sobie stronami.
2. **Certyfikat OV (Full Organization Validation)** – czyli certyfikat z weryfikacją właściciela. Oprócz powyższych danych wydawca podejmuje się także walidacji samego podmiotu, który ma otrzymać certyfikat. Tym samym będzie on zawierał nie tylko nazwę i dane firmy, ale i potwierdzał, że podmiot jest właścicielem serwisu. Certyfikatu OV nie można otrzymać bez złożenia dokumentów rejestrowych firmy, za to potrafi on zabezpieczyć większą liczbę domen.   
     
   Ten rodzaj certyfikatu jest nieco droższy niż typ DV, wymaga dodatkowych formalności, a jego wydanie trwa zazwyczaj 1-2 dni. Jest on najczęściej stosowany przez strony WWW, portale i sklepy internetowe.
3. **Certyfikat EV (Extended Validation)** – wersja z rozszerzoną weryfikacją właściciela certyfikatu. Najdroższy i wymagający największej cierpliwości, a jednocześnie najbardziej szczegółowy typ. Dany podmiot musi przed jego uzyskaniem przejść trzy stopnie weryfikacji. Wszelkie kryteria w tym zakresie są ustalane przez CA/Browser Forum. Sprawdzeniu ulegają: dane rejestrowe firmy, umowy spółki i samo prawo do posługiwania się domeną. Wszystkie te dane zostają potwierdzone dzięki rozmowie przez telefon, a jeśli firma ma niecałe trzy lata, weryfikuje się także rachunek bankowy. Strony, które zostały zabezpieczone certyfikatem EV, posiadają zielony pasek adresu w przeglądarce oznaczony dodatkowo nazwą firmy.   
     
   Tak dokładna weryfikacja tożsamości skutecznie podnosi poziom zaufania klientów. Rozpoznawalny zielony pasek przekłada się na zainteresowanie ofertą i na zwiększoną sprzedaż. Jednocześnie nie są to sprawy tanie – ceny certyfikatów EV zaczynają się od 1000 złotych, a otrzymuje się je dopiero po kilku, nawet 10 dniach. Ubiegają się więc o niego duże firmy, banki i sklepy internetowe
4. **Zastosowanie HTTPS w witrynach internetowych**

### 1. Ochrona Danych Użytkowników:

* Loginy i Hasła: Bezpieczna transmisja danych logowania.
* Formularze: Zabezpieczenie informacji przesyłanych przez formularze.

### 2. Bezpieczne Transakcje Finansowe:

* Sklepy Online: Zapewnienie bezpiecznych transakcji kartą kredytową.
* Bankowość Elektroniczna: Ochrona danych bankowych użytkowników.

### 3. Zarządzanie Sesjami Użytkownika:

* Ciasteczka (Cookies): Bezpieczna wymiana informacji o sesjach.
* Zabezpieczenie Przed Atakami: Unikanie kradzieży sesji.

### 4. Wrażliwe Dane Medyczne i Osobiste:

* Platformy Medyczne: Bezpieczna transmisja informacji medycznych.
* Dane Osobiste: Ochrona prywatności użytkowników.

### 5. SEO i Widoczność Wyszukiwarki:

* Wzrost Pozycji w Wynikach Wyszukiwania: Google preferuje witryny zabezpieczone.
* Wsparcie dla HTTP/2: Poprawa szybkości ładowania strony.

### 6. Zaufanie i Konwersje:

* Widoczność Zabezpieczeń: Symbol zamka w pasku adresu.
* Wiarygodność Marki: Użytkownicy bardziej skłonni do konwersji.

### 7. Platformy Społecznościowe i Udostępnianie Linków:

* Unikanie Problemów z Mieszaną Zawartością: Bezpieczne udostępnianie linków.
* Poprawa Widoczności: Lepszy wygląd linków na platformach społecznościowych.