Bogdan Roxana, sg 1.1

TEMA 1 DATC

HTTP vs. HTTPS

HTTP sau HyperText Transfel Protocol este un protocol de nivel de aplicație ce se focusează mai mult pe modul în care informația este prezentată clientului și mai putin pe modul în care acesta este transmisă din punctul A in punctul B. Toate datele sunt trimise de la browser la website ca “plain text” ceea ce face datele personale sau parolele utilizatorului vizibile pentru oricine poate sparge conexiunea dintre Website și server.

HTTPS înseamnă Hypertext Transfer Protocol și este identic cu HTTP în multe moduri, deoarece folosesc aceleași protocoale de bază. Atât HTTP cât și HTTPS folosesc acelasi Uniform Resource Identifier (URI), însa HTTPS este versiunea securizată ce cripteaza conexiunea realizată între browser și server.

HTTP funcționează în mod implicit pe portul 80, ceea ce înseamnă că calculatorul trebuie să trimită și să primească date prin acest port când utilizează HTTP, iar HTTPS folosește portul 443. Portului este doar un număr și nu prezintă nici o garanție a securității conexiunii. Spre exemplu, *http://example.com:443* este mai putin sigur decât *https://example.com:80*.

Cum functioneaza HTTPS?

Paginile HTTPS folosesc de obicei unul din cele două protocoale securizate pentru criptarea comunicațiilor - SSL (Secure Sockets Layer) sau TLS (Security Layer Security). Atât protocoalele TLS cât și SSL utilizează ceea ce este cunoscut ca un sistem de infrastructură cu cheie publică "asimetrică". Sistemul asimetric utilizează două "chei" pentru a cripta comunicațiile, o cheie "publică" și o cheie "privată". Orice codificare cu cheia publică poate fi decriptat numai de cheia privată și vice-versa.

După cum sugerează numele, cheia "privată" ar trebui să fie strict secreta, iar proprietarul cheii ar trebui să fie protejat. În cazul unui site web, cheia privată rămâne în siguranță pe serverul web. iar cheia publică este destinată distribuției.

Ce este un certificat?

Când solicitați o conexiune HTTPS la o pagină web, site-ul web va trimite inițial certificatul SSL în browser. Acest certificat conține cheia publică necesară pentru a începe sesiunea securizată. Pe baza acestui schimb inițial, browserul și site-ul dvs. inițiază apoi "strângerea de mână SSL". Handshake-ul SSL implică generarea de secrete partajate pentru a stabili o legătură unică între dvs. și site-ul web. Certificatul este un cod complex și unic creat special pentru user sau un Website. Certificatele trebuie achizitionate de la furnizori autorizați și de încredere (precum Comodo, VeriSign). Certificatele pot fi achizitionate de oriunde, pot fi chiar făcute de tine, dar sunt sigure?

Când se utilizează un certificat digital SSL de încredere în timpul unei conexiuni HTTPS, utilizatorii vor vedea o pictogramă cu un lacăt în bara de adrese a browserului.