

ПОЧЕМУ КАЖДОМУ ВЕБ-САЙТУ НУЖЕН HTTPS?

Т.Д. Позняков

Прежде всего, что означает использование веб-сайтом HTTPS, а не просто старого HTTP? Это означает, что сайт защищен SSL (Secure Sockets Layer) или более поздним TLS (Transport Layer Security). Если вы не осведомлены в этой теме, это заявление может ничего для вас не значить, так что давайте разберемся. При посещении сайта и использовании URL-адреса https запрашивается защищенная версия сайта. Короче говоря, это означает, что ваш браузер надеется увидеть сертификат SSL/TLS на сервере веб-сайта. Этот сертификат должен быть предоставлен проверяемым центром сертификации (ЦС) и в основном позволяет вашему браузеру взаимодействовать с ним через зашифрованное соединение. В зависимости от сертификата, на нем также может быть написано: «Смотрите, этот сайт – это тот, кто он говорит, что он был проверен». После того как этот сертификат будет найден, между вашим браузером и веб-сайтом может быть установлено безопасное зашифрованное соединение. Теперь, если кто-то попытается вмешаться и перехватить вашу связь, данные будут

зашифрованы. Возможно, ваш интернет-провайдер сможет определить, на какой веб-сайт вы заходили, или сколько данных передается туда и обратно, но дальнейшего отслеживания не будет. Если сервер веб-сайта принимает HTTPS-запросы, но для этого веб-сайта нет действительного сертификата или истек срок действия сертификата сайта, у него недействительный ЦС или любая другая проблема, браузер уведомит вас и попытается предотвратить продолжение работы. Это связано с тем, что сайт говорит, что есть защищенное подключение доступно, но не предоставляет его, поэтому браузер пытается сделать так, чтобы вы знали об этом.

Многие веб-серверы либо имеют сертификат, либо маршрутизируют весь входящий трафик по протоколу HTTPS, заставляя использовать безопасную версию, либо, если у них нет сертификата, маршрутизируют весь трафик по протоколу HTTP, тем самым предотвращая попытки пользователей получить доступ к несуществующему безопасному соединению.

Литература

1. Stephen A. Thomas. HTTP Essentials: Protocols for Secure, Scaleable Web Sites.
2. Krishnamurthy B., Rexford J. Web Protocols and Practice: HTTP/1.1, Networking Protocols, Caching, and Traffic Measurement.