digicert®

Ihre Kurzübersicht zu HTTPS Everywhere

Als einer der führenden Anbieter von SSL-Zertifikaten möchte DigiCert Sie über die Vorteile von HTTPS für Ihre gesamte Website informieren und Sie bei der erfolgreichen Implementierung unterstützen.

https:// Was ist HTTPS Everywhere?

HTTPS Everywhere ist ein optimales Sicherheitsverfahren für Websites, das Benutzer bei ihrem ganzen Online-Erlebnis vor Bedrohungen schützt. Der Begriff bezieht sich auf die Verwendung von HTTPS, dem sicheren, von SSL/TLS aktivierten Internetprotokoll, über Ihre ganze Website hinweg und nicht nur für bestimmte Teile der Website.

HTTPS authentifiziert die Identität, Verbindung und Datenintegrität der Website und verschlüsselt alle Informationen, die zwischen der Website und den Benutzern ausgetauscht werden, einschließlich aller Cookies, und schützt die Daten dadurch vor unbefugtem Zugriff, Manipulation und Missbrauch. Eine sichere Verbindung während der ganzen Browsersitzung ist von entscheidender Bedeutung für den Schutz der Benutzer vor Spoofing, Injektion und „Man-in-the-Middle"-Angriffen.

Browser und die Durchsetzung von HTTPS

Nur einen Teil der Benutzerverbindungen zu schützen, ist nicht länger akzeptabel. Wenn Sie HTTPS auf Ihrer Website nur teilweise einsetzen, dann sind nur gewisse Seiten durch die Verschlüsselung und Authentifizierung über SSL geschützt, während andere für Datendiebstahl, Injektion und Modifikation von Inhalten sowie Datenschutzverletzungen durch Internetüberwachung anfällig sind.

Eine teilweise Implementierung von SSL entspricht nicht den Erwartungen und Rechten der Benutzer in Bezug auf Sicherheit und erfüllt auch nicht die Erwartungen der Browser und Betriebssystemplattformen. Im Rahmen eines mehrjährigen Vorhabens, den Einsatz von HTTPS zu fördern, haben gängige Browseranbieter wie Google, Mozilla und Apple langsam Änderungen an der Benutzeroberfläche ihrer Browser vorgenommen, um HTTP negativ zu verstärken und das sichere HTTPS zu fördern.

Warum ist das wichtig?

Online-Geschäfte beruhen auf Kundenvertrauen. Um dieses Vertrauen zu gewinnen, sollten Sie jede Seite schützen, die Ihre Besucher aufrufen, nicht nur die Anmeldeseite und den Warenkorb. Neue Änderungen in den Internetstandards und Webbrowsern bevorteilen Websites, die HTTPS verwenden, und bestrafen die nicht gesicherten Websites, die bei HTTP bleiben.

Google zum Beispiel vermittelt seit 2014 den Suchergebnissen der Seiten, die über HTTPS zugänglich sind, einen Ranking-Vorteil. Google zeigt auch einen „Sicher"-Hinweis in der Adressleiste für HTTPS-Seiten an. Und ab Juli 2018 zeigt Google Chrome eine „Nicht sicher"-Warnung für jede Seite, die über HTTP bereitgestellt wird. Chrome ist

der erste gängige Browser, der Benutzer auf allen HTTP-Seiten warnt, und andere Browser werden folgen. Dies geschieht im Rahmen des Übergangs des Internets zu einer standarmäßigen Sicherheitsnorm.

Außerdem verlangen viele neue Internettechnologien und Browserfunktionen das HTTPS-Protokoll. Dazu gehört HTTP/2, ein von Grund auf verbessertes Internetkommunikationsprotokoll, das die Website-Performance bedeutend steigern kann, sowie Browserfunktionen, unter anderem Geolokalisierung, Benachrichtigungen, Service Worker, AMP-Mobilstandard von Google, neue Komprimierungsmethoden und mehr. Kurz gesagt, ohne HTTPS wird Ihre Website in der Vergangenheit gefangen sein.

3 Die drei wichtigsten Tipps für die Umstellung auf HTTPS Everywhere

1. Vergewissern Sie sich, dass alle Services von Drittanbietern, von denen Sie abhängig sind, wie Werbung oder Analysedienste, auf Ihrer Website über HTTPS verfügbar sind, um Probleme mit „gemischten Inhalten“ zu vermeiden.
2. Kaufen Sie zusätzliche SSL-Zertifikate, falls verschiedene Teile Ihrer Website auf unterschiedlichen Servern oder Domänen ausgeführt werden.
3. Leiten Sie alle Ihre Seiten zu ihren neuen HTTPS-Seiten um und aktualisieren Sie Ihre Google Webmaster-Tools. Wenn Sie auf HTTPS Everywhere umstellen, hat dies einen Einfluss auf SEO. Google und andere Suchmaschinen betrachten dies als eine Verschiebung der Website, ähnlich wie eine Verschiebung zu einem neuen Domänennamen.

digicert®

Fazit

- HTTPS Everywhere auf Ihrer Website schützt den Benutzer und die Daten Ihres Unternehmens auf jeder Seite, von Anfang bis Ende.
- Der teilweise Einsatz von SSL-Verschlüsselung reicht heute nicht mehr aus, um die Besucher Ihrer Website zu schützen und den Diebstahl vertraulicher Daten zu verhindern.
- Browserbenutzeroberflächen beginnen, negative „Nicht sicher“-Indikatoren für HTTP-Seiten anzuzeigen, und dieser Trend wird sich aufgrund der erhöhten Anforderungen an die Sicherheit fortsetzen.
- Verbessern Sie Ihr Google-SEO-Ranking mit HTTPS Everywhere, ein Vorteil, der in Zukunft noch ausschlaggebender sein wird.
- HTTPS Everywhere lässt sich für Ihre Website leicht implementieren und erfordert keine zusätzliche Hardware.
- Sichern Sie Ihre Website mit SSL-Zertifikaten, um Ihre Marke und Ihren Ruf zu stärken, indem Sie zeigen, dass Ihnen die Online-Sicherheit wichtig ist.
- Größeres Kundenvertrauen führt zu niedrigeren Bounce-Raten und weniger abgebrochenen Einkäufen. Dadurch steigen die Abschlussraten und die Anzahl der abgeschlossenen Transaktionen.