SSL-Zertifikat: mehr Sicherheit für Ihre Webseite

Schützen Sie Ihre Website mit SSL und HTTPS

Unser Leben spielt sich zunehmend online ab. Es gehört zu unserem Alltag, Waren oder Dienstleistungen im Internet zu kaufen oder buchen. Dabei geben wir viele sensible Daten preis. Wir melden uns mit persönlichen Angaben auf Websites an, nennen Bankverbindungen, Passwörter oder Krankenkassendaten oder hinterlegen Kreditkartennummern. Zugleich steigt die Zahl der Hacker und Datendiebe. Online-Betrug und Fälle von Identitätsdiebstahl lassen immer mehr Kunden davor zurückschrecken, persönliche Daten auf unbekannten Websites anzugeben.

Als Betreiber einer Internetseite müssen Sie die Geheimhaltung sensibler Kundendaten gewährleisten. Ein SSL-Zertifikat für Ihre Domain zeigt den Kunden, dass Ihre Internetseite sicher ist. Eine SSL-Verschlüsselung sichert die Geheimhaltung Ihrer Online-Kommunikation und versichert Ihren Kunden, dass es sich bei der besuchten Seite auch tatsächlich um Ihre handelt. Mit einem SSL-Zertifikat stellen Sie gesicherte Verbindungen her und stärken das Vertrauen Ihrer Online-Kunden in Ihre Homepage

Was ist ein SSL-Zertifikat?

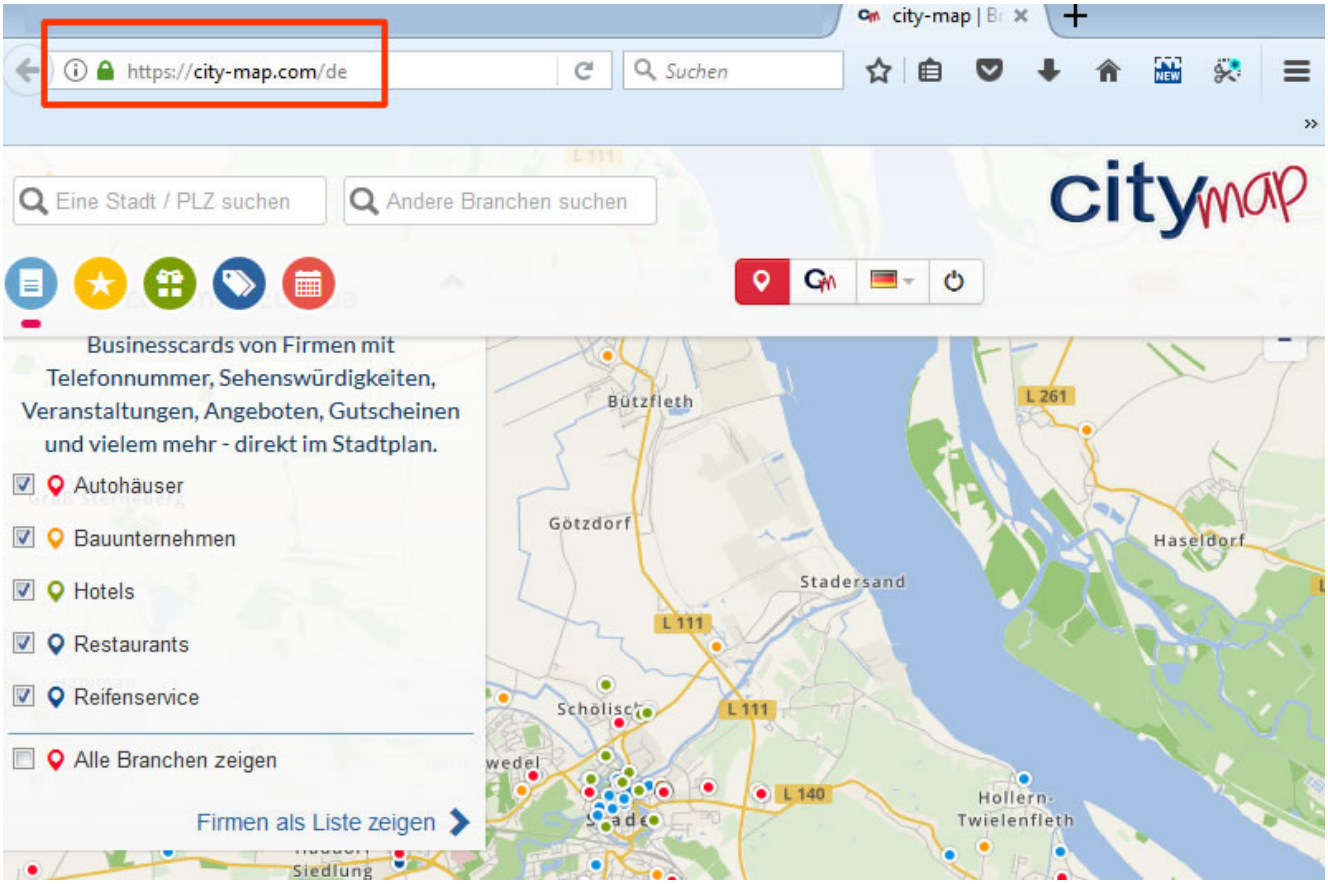
SSL steht für „Secure-Sockets-Layer“. Ein SSL-Zertifikat sorgt dafür, dass Ihre Webseite verschlüsselt aufgerufen werden kann und eine gesicherte Verbindung für Ihre Kunden besteht. Im Prinzip ist ein SSL-Zertifikat nichts anderes als ein Code, der für eine Domain eingebunden wird und die Geheimhaltung Ihrer Online-Kommunikation garantiert. Er verschlüsselt die

Datenübertragung zwischen Web-Browser und Server. Die Details dieser Verschlüsselung führt das entsprechende SSL-Zertifikat auf. Oder anders: Das SSL-Zertifikat verschlüsselt den Datenaustausch zwischen einem Server und dem darauf zugreifenden Computer. Es garantiert den Besuchern einer Internetseite den Schutz ihrer Daten vor dem Zugriff durch Dritte.

Jedes SSL-Zertifikat gewährleistet die Geheimhaltung sensibler Kundendaten und enthält zudem detaillierte Identifizierungsinformationen. Wer ein SSL-Zertifikat anfordert, erfährt von einer Drittpartei die Verifikation seiner Daten und bekommt ein nur für ihn bestimmtes Zertifikat, das seiner Authentifizierung dient. Ein SSL-Zertifikat belegt, dass Sie auch tatsächlich der Betreiber der Webseite sind und stärkt somit das Vertrauen Ihrer Kunden in Ihre Internetseite.

Wie erkennt der Nutzer, ob die Internetseite sicher ist?

Ob SSL für eine Webseite aktiv ist, zeigt ein kleines Schloss-Symbolbild, das ganz links in der Adresszeile des Internetbrowsers zu sehen ist. Es zeigt zugleich an, welche Art von SSL-Zertifikat die Webseite nutzt.

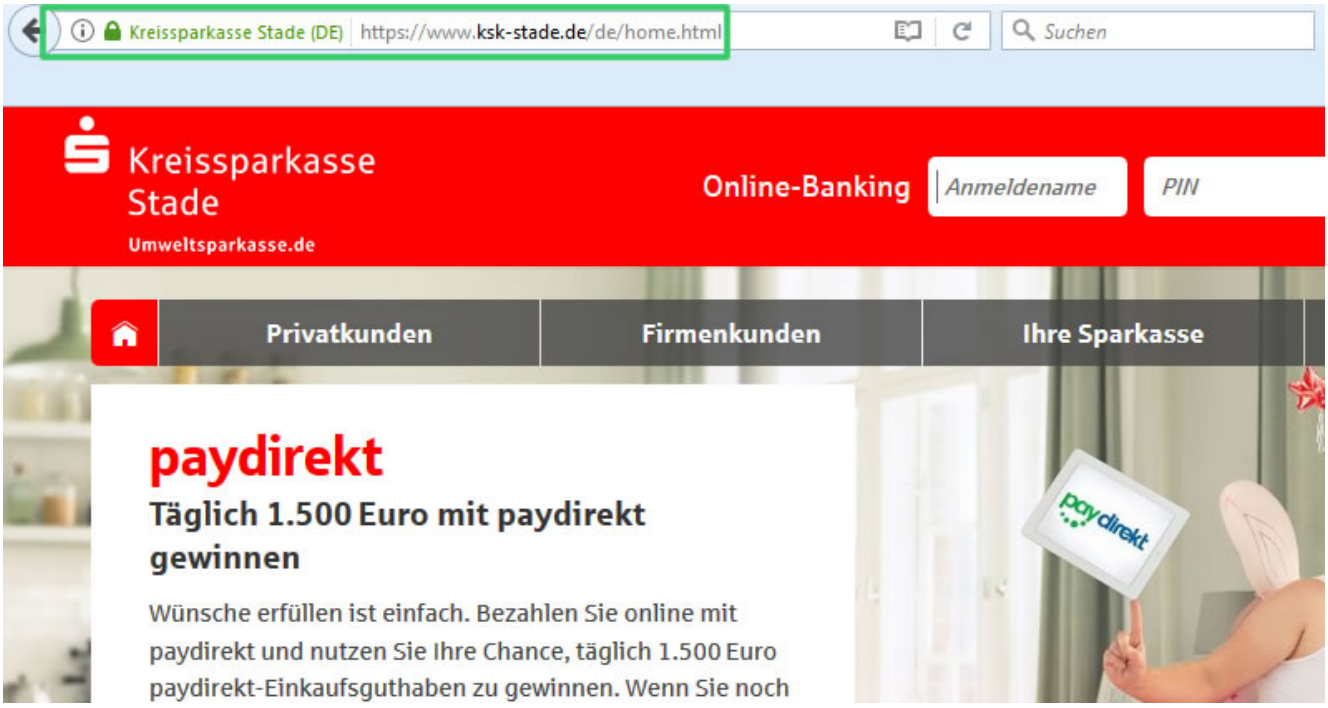


SSL-Zertifikate enthalten verifizierte Informationen zur gesicherten Internetseite, sodass die User sicher sein können, auch tatsächlich auf Ihre Webseite zuzugreifen. Es gibt drei verschiedene Möglichkeiten einer SSL-Verschlüsselung, die jeweils unterschiedliche Anforderungen an den Betreiber stellen:

- Domain-Validated-Zertifikat (DV-SSL)
- Organisation-Validation-Zertifikat (OV-SSL)
- Extended-Validation-Zertifikat (EV-SSL)

Ein Extended-Validation-Zertifikat bietet Internetnutzern den höchsten Verifizierungsstandard und die größte Transparenz zum Thema Sicherheit für potenzielle Besucher der gesicherten Seite.
Eine Website mit einem EV-SSL-Zertifikat ist daran zu erkennen, dass der Firmenname ebenfalls in der Adresszeile steht und grün gefärbt ist (siehe Screenshots zur Kreissparkasse Stade). Die anderen beiden Zertifikate sind in ihrer grafischen Darstellung auf den ersten Blick nicht

voneinander zu unterscheiden. Wer allerdings auf das Schloss-Symbol klickt, erhält weitere Informationen zum aktiven SSL-Zertifikat. Ein OV-SSL-Zertifikat zeigt Informationen zum Betreiber der Webseite, das DV-Zertifikat hingegen nicht.



Screenshot Kreissparkasse Stade | https://www.ksk-stade.de | mit Extended-Validation-Zertifikat (EV-SSL)

Wer benötigt ein SSL-Zertifikat?

SSL-Zertifikate garantieren die Geheimhaltung sensibler Daten im Internet. In erster Linie dienen SSL-Zertifikate dazu, das Vertrauen Ihrer Kunden in die Sicherheit Ihrer Internetseite zu stärken. Wer online vertrauliche Daten wie Bankdaten oder Adressen eingibt, muss sich darauf verlassen können, dass diese nicht von Dritten eingesehen und schlussendlich missbraucht werden können. Zugleich bestätigt ein aktives SSL-Zertifikat Ihren Kunden, dass Sie auch tatsächlich der Betreiber der besuchten Webseite sind.

Zu den persönlichen Daten, die in jedem Fall durch eine SSL-Verschlüsselung geschützt werden sollten, gehören zum Beispiel Angaben zur Registrierung auf einer Internetseite (Namen,

Adressen, Telefonnummern), Log-in-Daten wie Passwörter und E-Mail-Adressen oder Zahlungsinformationen wie Bankverbindungsdaten oder Kreditkartennummern.
SSL-Verschlüsselungen kommen darüber hinaus bei E-Mail-Servern, internetbasierten Anwendungen wie Kontaktformularen und der Kommunikation zwischen Servern zur Anwendung.

Als Betreiber einer Internetseite benötigen Sie ein SSL-Zertifikat, wenn…

- Sie einen Online-Shop betreiben und Online-Bestellungen akzeptieren.
- Sie auf Ihrer Webseite Formulare – und Kontaktformulare Daten übertragen.
- Sie persönliche Daten wie Namen, Adressen oder Bankdaten übertragen oder verwalten.

Wie funktioniert ein SSL-Zertifikat?

Ein aktives SSL-Zertifikat bietet den Besuchern einer sicheren Internetseite authentifizierte Informationen zur Identität des Webservers. Zugleich stellt eines in wenigen Augenblicken eine sichere, verschlüsselte Verbindung her.

So läuft der Austausch zwischen einem Webbrowser und dem zertifizierten Server ab:

1. Sobald ein Webbrowser eine Verbindung mit einer SSL-gesicherten Internetseite herzustellen versucht, fragt der Browser nach der Identität des Webservers.
2. Dieser sendet daraufhin eine Kopie seines SSL-Zertifikats zurück an den Internetbrowser.
3. Beurteilt der Browser das SSL-Zertifikat für glaubwürdig, sendet er wiederum eine Nachricht an den Server.
4. Der Server leitet die SSL-gesicherte Verbindung ein,

indem er eine digital signierte Bestätigung an den Browser zurückschickt.
5. Browser und Server tauschen in einer gesicherten Verbindung verschlüsselte Daten aus.

Was ist HTTPS?

HTTPS steht für „Hypertext Transport Protocol Secure“ und ist letztlich das **Protokoll Ihrer sicheren Datenübertragung.** HTTP hingegen bezeichnet eine nicht durch SSL-Zertifikat abgesicherte Variante. Theoretisch können bei HTTP-Websites ohne SSL-Zertifikat alle übertragenen Daten von unberechtigten Dritten mitgelesen. In diesem Fall kann der Internetnutzer sich nicht sicher sein, dass er seine sensiblen Daten wie Kreditkarteninformationen oder Bankverbindungen tatsächlich an einen Internetshop übermittelt – oder womöglich an einen kriminellen Hacker. SSL verschlüsselt die HTTP-Daten und garantiert dem User die Geheimhaltung seiner Daten. Das SSL-Zertifikat bzw. das weiterentwickelte **TLS-Zertifikat schützt die Online-Kommunikation vor dem Zugriff durch Dritte**. Mittlerweile wird nahezu ausschließlich der Einsatz von TLS empfohlen – wer von SSL spricht, meint tatsächlich meist TLS.

Ihre SSL-(TSL-)Vorteile auf einen Blick:

- Datenschutz für Ihre Online-Kunden und Partner
- Deutliche Minimierung des Risikos von Datenmissbrauch
- Positive Auswirung auf Ihr Google-Ranking
- SSL-Zertifikat stärkt das Vertrauen der Online-Nutzer
- Nutzung von HTTP/2 zur Verbesserung der Internetseiten-Performance möglich

FAZIT: Schützen Sie Ihre Website mit SSL und HTTPS

Neue Internetseiten sollten von vornherein eine SSL-Verschlüsselung haben. Doch auch für bereits bestehende Internetseiten bedeutet es keinen großen Aufwand, auf HTTPS umzustellen. Erwerben Sie ein SSL-Zertifikat für Ihre Domain.

Dieses dient als Nachweis der Identität einer Internetseite. Die SSL-Zertifikats-Vergabestelle prüft Ihre Identität und bürgt nach der Vergabe für die Korrektheit Ihrer Angaben. Immer dann, wenn ein Internetnutzer eine Website mit HTTPS aufruft, wird das SSL-Zertifikat vom Server abgerufen.

Ein Beitrag von Saleema Schönwald
Leiterin – Online Business Performance
city-map Stade

Sie benötigen weitere Infos zu SSL und HTTPS? Dann nehmen Sie Kontakt mit uns auf!