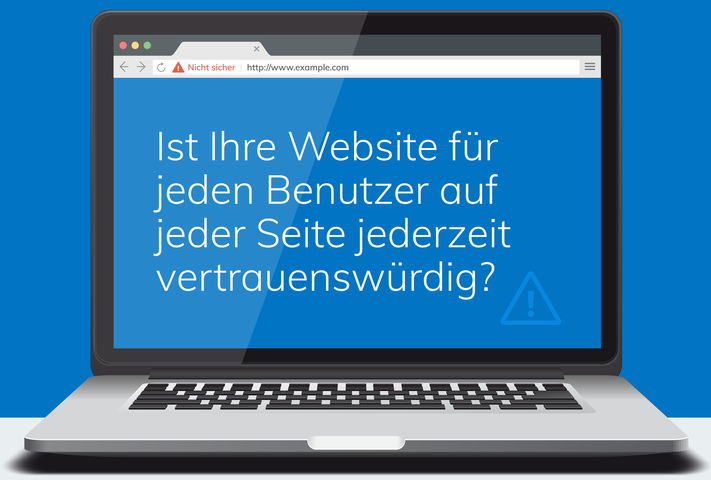
digicert



Sicherheitsänderungen für die Website zählen zu den wenigen Konstanten im modernen Internet. Mit den richtigen Zertifikaten für Ihre Website und für jede Webseite sind Sie auf laufende Updates vorbereitet.

Ist Ihre Website davon betroffen?

Google Chrome und Mozilla Firefox warnen Benutzer bereits, wenn Webseiten Anmeldeinformationen oder Kreditkartendaten abfragen, ohne SSL-Zertifikate zu verwenden. Und im Juli 2018 wird Google Chrome der erste Browser sein, der Benutzern für jede Seite Ihrer Website, die nicht mit einem SSL-Zertifikat gesichert ist, eine deutliche „Nicht sicher"-Warnung anzeigt.

Wie sieht diese Warnung aus?

Seiten ohne SSL-Zertifikate

CHROME (AKTUELLE VERSION):
Webseite verlangt KEINE Angabe von Anmelde- oder Kreditkartendaten.

CHROME (AKTUELLE VERSION):
Webseite VERLANGT die Angabe von Anmelde- oder Kreditkartendaten.

CHROME 68 (JULI):
ALLE Webseiten

Das richtige Zertifikat kann ausschlaggebend sein.

Zwar bieten alle SSL-Zertifikate das gleiche Verschlüsselungsniveau, aber hochsichere Zertifikate bieten zusätzliche Authentifizierungsebenen, um Benutzern zu beweisen, dass sie Ihnen vertrauen können. Dies stärkt das Vertrauen für Ihre ganze Website. Hier ist ein Vergleich der Zertifikate.

Domänenvalidierung (DV)

WICHTIGE UNTERSCHEIDUNGSMERKMALE:
- Schnellste Ausstellung
- Keine Firmenangaben auf dem Zertifikat
- Leichteres Abfangen für Phishing-Websites

BENUTZERPERSPEKTIVE:

„Ich befinde mich auf einer Website, die sicher zu sein scheint."

ÜBERPRÜFT:

Besitz/Kontrolle der Domäne

NORMALERWEISE VERWENDET FÜR:
- Interne/nicht öffentlich zugängliche Websites
- Webbasierte Anwendungen (kein Betrugsrisiko)
- Für Websites, bei denen Vertrauenswürdigkeit weniger wichtig ist als Datensicherheit

Unternehmensvalidierung (OV)

WICHTIGE UNTERSCHEIDUNGSMERKMALE:
- Stärkere Zusicherung mit mehr Optionen, um die Legitimität der Website anzuzeigen
- Validierte Unternehmensangaben im Zertifikat angegeben

BENUTZERPERSPEKTIVE:

„Ich bin auf einer gesicherten Website, die einem seriösen Unternehmen gehört."

ÜBERPRÜFT:

Besitz/Kontrolle der Domäne

Zusätzliche Informationen über das Unternehmen, das die Kontrolle über die Website hat (registrierter/gesetzlicher Name, Standort usw.)

NORMALERWEISE VERWENDET FÜR:
- Öffentlich zugängliche Websites für Transaktionen mit weniger sensiblen Daten
- Durchsuchbare Informations-Websites
- Websites von Behörden und Bildungseinrichtungen

Extended Validation (EV)

WICHTIGE UNTERSCHEIDUNGSMERKMALE:
- Höchste Sicherheit mit der stärksten sichtbaren Bestätigung der Identität
- Grün eingefärbte Adressleiste mit dem Namen des Unternehmens
- Umfassend überprüfte Informationen, im Zertifikat angegeben

BENUTZERPERSPEKTIVE:

„Dieser gesicherten Website kann ich meine sensibelsten persönlichen Daten anvertrauen."

ÜBERPRÜFT:

Besitz/Kontrolle der Domäne

Zusätzliche Informationen über das Unternehmen, das die Kontrolle über die Website hat (registrierter/gesetzlicher Name, Standort usw.)

Umfassende identifizierende Details (rechtlicher Status, physische und betriebliche Existenz, Berechtigung zum Unterschreiben von Verträgen usw.) über strikte Querverweise zu externen Quellen

NORMALERWEISE VERWENDET FÜR:
- Websites, die eine Anmeldung verlangen, Zahlungen annehmen oder private Informationen oder andere sensible Daten verarbeiten, z. B. Websites für E-Commerce, Banking und das Gesundheitswesen
- Websites, die das Vertrauen ihrer Besucher mit einem visuellen Kennzeichen in der Adressleiste stärken wollen

Es geht um mehr als nur um HTTPS.

Hochsichere OV- oder EV-SSL auf jeder Seite sorgen dafür, dass Benutzer Ihre Website leicht als authentisch erkennen können, was das Imitieren durch Phishing-Websites und das Betrügen Ihrer Besucher erschwert.

Wenden Sie sich noch heute an einen Kundenbetreuer für eine vollständige Website-Überprüfung.