Factsheet SSL

Was ist SSL?

SSL (Secure Sockets Layer), auch bekannt als TLS (Transport Layer Security), ist ein Schlüsselprotokoll für die Sicherheit von Anwendungen. Es verschlüsselt die Datenübertragung zwischen Nutzern und Servern, um die Vertraulichkeit und Integrität sensibler Informationen zu schützen. Dies minimiert das Risiko von Cyberangriffen wie Man-in-the-Middle und ist besonders wichtig für die Sicherheit von Webanwendungen.

HTTP vs HTTPS

Merkmal	HTTP	HTTPS
Port	80	443
Sicherheit	Anfällig für Abhören und Datenmanipulation	Schützt vor Abhören und Manipulation durch Verschlüsselung
Datenschutz	Daten sind für Dritte sichtbar	Daten sind verschlüsselt und für Dritte nicht lesbar
Vertrauenswürdigkeit	Keine visuellen Sicherheitsindikatoren in Browsern	Von Browsern mit Schloss- Symbol als sicher gekennzeichnet
SEO-Vorteile	Keine	Wird von Suchmaschinen bevorzugt
Verschlüsselung	Keine	Verwendet SSL/TLS zur Verschlüsselung der Daten

SSL-Zertifikate

SSL-Zertifikate (Secure Sockets Layer) sind digitale Zertifikate, die die Sicherheit der Datenübertragung über das Internet gewährleisten. Sie ermöglichen eine verschlüsselte Verbindung zwischen einem Webserver und einem Browser und sichern so die Daten, die zwischen diesen beiden Punkten ausgetauscht werden. SSL-Zertifikate enthalten Informationen über den Inhaber des Zertifikats, wie zum Beispiel den Namen und die Adresse, sowie den öffentlichen Schlüssel und die Signatur der ausstellenden Zertifizierungsstelle, die die Authentizität des Zertifikats bestätigt. Dies hilft dabei, die Identität der Website zu verifizieren und schützt Nutzer vor Man-in-the-Middle-Angriffen, bei denen Angreifer Daten abfangen könnten.

Probleme und Risiken

- Man-in-the-Middle-Angriffe
- Datendiebstahl
- Compliance-Verletzungen
- Reputationsschaden
- Session-Hijacking

Best Practices

- Starke Verschlüsselungsalgorithmen
- Neueste Protokollversionen
- Zertifikatsvalidierung
- Perfect Forward Secrecy (PFS) aktivieren
- Endpunktkonfiguration testen
- Verschlüsselung auf mehreren Ebenen

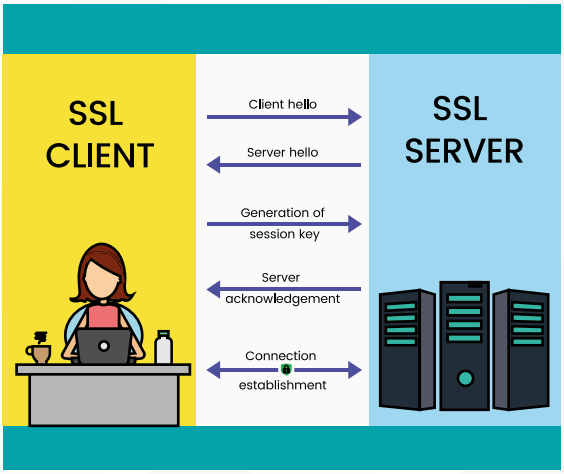
Let's Encrypt

Let's Encrypt ist eine gemeinnützige Zertifizierungsstelle, die 2014 gegründet wurde, um die Verbreitung von SSL/TLS-Zertifikaten zu fördern, damit Websites sichere HTTPS-Verbindungen anbieten können. Diese Organisation ermöglicht es Webseitenbetreibern, kostenlos und automatisch SSL-Zertifikate zu erhalten. Dies ist besonders wichtig, um die Datenübertragung im Internet sicherer zu gestalten, indem verschlüsselte Verbindungen zur Standardmethode werden. Let's Encrypt hat die Implementierung von HTTPS durch seine einfache Integration und die Automatisierung des Erneuerungsprozesses der Zertifikate revolutioniert, was die allgemeine Internetsicherheit erheblich verbessert hat.

Let's Encrypt

Fakten

- 94,3% der SSL-Zertifikate sind Domain Validation
- Über 90 % aller Phishing-Websites verwenden HTTPS
- 35,4 % des unverschlüsselten Datenverkehrs stammt von mobilen Geräten
- 96,3 % aller SSL-Zertifikate im Internet werden von nur 9 Zertifizierungsstellen ausgestellt
- Deutschland verfügt über fast 14 Mio. Zertifikate
- Tschad dagegen verfügt nur über 125



Maurice Däppen & Patrick Aeschlimann