HTTPS Checkliste

Version 1.0 (26.08.2015)

Inhaltsverzeichnis

Best Practices

1 Private Key und Zertifikat

1.1 2048-Bit Private Keys

Der Private Key legt den Grundstein für die Sicherheit und das Zertifikat.

Verwenden Sie hier also mindestens eine 2048 Bit Verschlüsselung.

1.2 Geheimhalten der Private Keys

Halten Sie Ihre Private Keys geheim und geben Sie nur einer begrenzten Anzahl von Personen Zugriff auf diese.

Folgende Richtlinien sollten ebenfalls eingehalten werden:

- Privater Schlüssel und Certificate Signing Request sollten auf einem vertrauenswürdigen Computer erstellt werden.
- Einige CAs bieten an die Schlüssel zu erstellen. Hiervon ist abzuraten.
- Wenn Zertifikate erneuert werden, sollten immer neue Schlüssel generiert werden.
- Ausreichende Abdeckung von Hostnamen

1.3 Ausreichende Abdeckung von Hostnamen

Stellen Sie sicher, dass Ihr Zertifikat alle benötigten Hostnamen abdeckt.

Es ist zu verhindern das durch nicht abgedeckte Hostnamen eine Zertifikatswarnung erscheint.

1.4 Zertifikat von einer vertrauenswürdigen CA

Achten Sie bei der Auswahl eines Zertifikat Anbieters darauf, dass Sie einen zuverlässigen Partner wählen.

1.5 Verwenden von sicheren Algorithmen

Die Sicherheit hängt unter anderem von Verschlüsselungsstärke und den verwendeten Algorithmen ab. Die meisten Zertifikate nutzen aktuell die SHA1 Hash-Funktion, welche als unsicher klassifiziert ist. Achten Sie darauf das mindestens die SHA2 Hash-Funktion genutzt wird. Aber achten Sie auf Ihre User. Einige ältere Clients unterstützen die SHA2 Hash-Funktion nicht.

2 Serverkonfiguration

2.1 Alle nötigen Zertifikate einbinden

In vielen Fällen muss mehr als ein Zertifikat in der Serverkonfiguration hinterlegt werden.

Ihr CA stellt gewöhnlich alle nötigen Zertifikate bereit.

2.2 Verwenden von sicheren Protokollen

In diesem Bereich existieren fünf Protokolle: SSL v2, SSL v3, TLS v1.0, TLS v1.1, TLS v1.2.

In der Verwendung mit HTTP(S) ist von den SSL Protokollen aufgrund von Sicherheitsproblemen abzuraten. Die TLS Protokolle können meist ohne Probleme verwendet werden.

2.3 Verwenden von sicheren Chiffren

Folgende Dinge sollten vermieden werden:

- Anonymous Diffie-Hellman (ADH) Suiten
- NULL Chiffren Suiten
- RC4 Chiffre
- Chiffren mit weniger als 128-Bit

2.4 Unterstützen von Forward Secrecy

Forward Secrecy ist eine Protokoll-Funktion die sichere Verbindungen unabhänging vom Privaten Schlüssel zulässt.

Bei Verwendung von Algorithmen die diese Funktion nicht unterstützen,

ist es möglich den Privaten Schlüssel zu berechnen und aufgezeichnete Verbindungen zu entschlüsseln.

2.5 Absichern bekannter Lücken

Folgende bekannte Lücken sollten geschlossen werden:

- Deaktivieren von TLS Komprimierung
- Deaktivieren des RC4 Algorithmus
- Absichern der BEAST Lücke
- Deaktivieren des SSLv3 Protokolls

3 Anwendung

3.1 Gesamte Anwendung verschlüsseln

Achten Sie darauf dass nicht nur die Webseite ein sich verschlüsselt übertragen wird, sondern auch alle weiteren eingebundenen Daten.

Dies betrifft auch JavaScript-, CSS- und Bilddateien.

Wichtig ist auch, Dateien von externen Quellen immer über HTTPS eingebunden werden.

3.2 Verwenden von HSTS

HTTP Strict Transport Security (HSTS) ist ein Mechanismus der sicherstellt, dass die betreffende Webseite immer über HTTPS und nicht im ersten Request über HTTP aufgerufen wird.

Hierbei muss ein entsprechender HTTP Header mitgesendet werden.

3.3 Deaktivieren des Cachings von sensiblen Inhalten

Stellen Sie sicher, das sensible Inhalte weder server- noch clientseitig gecached werden.

Checkliste

1 Private Key und Zertifikat

- ☐ Verwenden von 2048 Bit Private Keys
- ☐ Geheimhalten der Private Keys
- ☐ Ausreichende Abdeckung von Hostnamen
- ☐ Zertifikat von einer vertrauenswürdigen CA
- ☐ Verwenden von sicheren Algorithmen

2 Serverkonfiguration

- ☐ Alle nötigen Zertifikate werden eingebunden
- ☐ Verwenden von sicheren Protokollen
- ☐ Verwenden von sicheren Chiffren
- ☐ Forward Secrecy wird unterstützt
- ☐ Bekannter Lücken sind abgesichert

3 Anwendung

- ☐ Gesamte Anwendung verschlüsselt
- ☐ Verwenden von HSTS
- ☐ Deaktivieren des Cachings von sensiblen Inhalten