TRALIOS
Linux Server Management

Verschlüsselte Webseiten mit SSL – aber richtig

Wie setze ich SSL sinnvoll, kostengünstig und sicher ein?

Dominik Vallendor ■ 12.11.2018

Über mich

TRALIOS
Linux Server Management

- **Dominik Vallendor**
- Dipl.-Inform., Universität Karlsruhe
- Seit 1995: Internet / Linux
- Seit 2002: Selbständig
- Seit 2010: Tralios IT GmbH:
  sicheres und zuverlässiges
  Server Management und Hosting

Übersicht

TRALIOS
Linux Server Management

- Grundlagen
- Unterschiede
- Let's Encrypt
- Implementierung / Sicherheit
- Fazit

Einsatz von SSL

TRALIOS
Linux Server Management

Wofür wird SSL genutzt?

- Verschlüsselung von Datenverkehr im Internet
- Vor allem: Webseitenaufruf (https://)
- aber auch: FTPS, IMAPS, SMTPS, ...

Korrekte, neuere Bezeichnung eigentlich: **Transport Layer Security (TLS)**

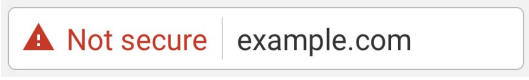
Achtung: **nicht** zu verwechseln mit

- SSH, SCP, SFTP, ...

Gründe für den Einsatz von SSL

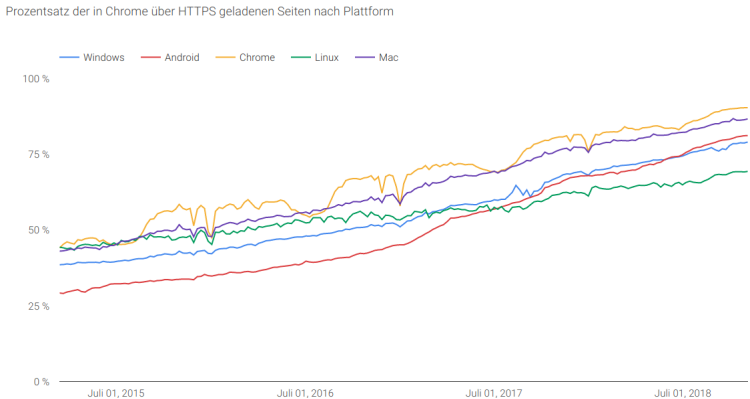
TRALIOS
Linux Server Management

- Sichere Datenübertragung: kein Mitlesen, keine Manipulation
- Rechtlich oft verpflichtend (DSGVO, Bsp. Kontaktformular)
- Warnmeldung bei nicht verschlüsselten Webseiten in aktuellen Browsern



- Besseres Ranking in Suchmaschinen (Google)
- Schnelles HTTP/2 oft nur mit SSL nutzbar

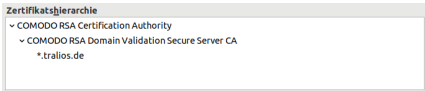
SSL ist inzwischen Standard

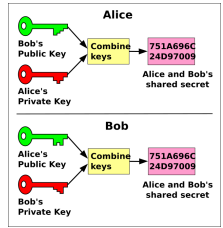


Quelle: https://transparencyreport.google.com/https/overview

Funktionsprinzip

- Schlüsselaushandlung (Diffie-Hellman)
- Server identifiziert sich durch Zertifikat
- Vertrauensanker im Browser hinterlegt
- Zwischenzertifikate





Quelle: Wikipedia

Ablauf der Zertifizierung

TRALIOS
Linux Server Management

- Erstellung eines geheimen Schlüssels (.key) und Certificate Signing Requests (.csr)
- Einreichen des CSR beim Aussteller
- Validierung durch den Aussteller
- Aussteller liefert Zertifikat (.crt) und Zwischenzertifikate
- Installation von Zertifikat, Zwischenzertifikaten und Key auf dem Server

Beispiel-Konfiguration Apache

TRALIOS
Linux Server Management

```
<VirtualHost *:443>
    ServerName www.example.com
        [...]
        SSLEngine on
        SSLCertificateFile /etc/ssl/server/example.crt
        SSLCertificateKeyFile /etc/ssl/server/example.key
        SSLCACertificateFile /etc/ssl/server/example.ca-bundle
</VirtualHost>
```

Unterschiede zwischen den SSL-Zertifikaten

TRALIOS
Linux Server Management

- Aussteller
- Art der Validierung
- Abgesicherte Domain/Subdomain(s)
- Laufzeit

Aussteller

TRALIOS
Linux Server Management

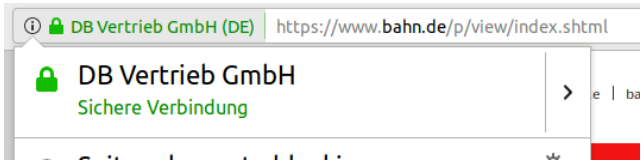
- sog. Certification Authority (CA)
- ca. 100 Firmen am Markt, davon ca. 10 gebräuchlich
- Preise und Zielgruppen sehr unterschiedlich
- Verkaufen teilweise Zusatzprodukte, z.B. Garantien/Versicherungen
- Unterschiedliche Browser-Akzeptanz
- Alternative: selbstsigniert (nur eingeschränkt)

Art der Validierung

TRALIOS
Linux Server Management

- **Domain Validation (DV)**: meist verwendet, **günstig**
- **Organization Validation (OV)**: mit Firmenangabe, aber kaum genutzt
- **Extended Validation (EV)**: bei hohem Vertrauensbedarf

  (Grüne) Adressleiste mit Firmenangabe



Abgesicherte Domains

TRALIOS
Linux Server Management

- **Domain/Subdomain**: Bsp. www.example.com oder example.com
- **Multidomain**: www.example.com UND shop.example.net UND blog.example.org
- **Wildcard**: ***.example.com - ACHTUNG: Wildcard NICHT für EV-Zertifikate

Preise:

- abhängig von der Anzahl der Domains
- Wildcard: ca. 3-5facher Preis des Standard-Zertifikats

Laufzeit

TRALIOS
Linux Server Management

- Maximal nur noch 2 Jahre (genauer: 825 Tage)
- Trend geht zu kürzeren Laufzeiten
- Klassische/Standard-Zertifikate: 1 oder 2 Jahre
- Test-Zertifikate: 30 Tage
- Let's Encrypt: 90 Tage

Neue Entwicklung: Let's Encrypt

TRALIOS
Linux Server Management

- Intiative zur stärkeren Verbreitung von SSL
- Kostenlose SSL-Zertifikate
- Vertrauensanker in allen Standardbrowsern vorhanden
- Automatisierte Validierung durch *Automatic Certificate Management Environment* (ACME)
- Laufzeit max. 90 Tage: manuelle Erneuerung daher nicht sinnvoll

Let’s Encrypt Clients

TRALIOS
Linux Server Management

Inzwischen dutzende Clients erhältlich. Beispiele:

- **Certbot**: Standard-Client
- **Traefik**: Proxy, insb. auch für Docker-Setups geeignet
- **mod_md**: Apache-Modul

Weitere Clients: https://letsencrypt.org/docs/client-options/

Beispiel-Konfiguation Traefik

TRALIOS
Linux Server Management

```
[acme]
email = "info@example.com"
storage = "/etc/traefik/acme.json"
entryPoint = "https"
onDemand = true

[acme.httpChallenge]
entryPoint = "http"
```

Beispiel-Konfiguation mod_md

TRALIOS
Linux Server Management

```
ServerAdmin mailto:info@example.com
MDCertificateAgreement https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf
MDNotifyCmd /etc/apache2/acmenotify.sh
MDRequireHttps temporary

MDomain www.example.com
<VirtualHost *:443>
    ServerName www.example.com
    [...]
    SSLEngine on
</VirtualHost>
```

Sicherheitsprobleme

TRALIOS
Linux Server Management

Zahlreiche Sicherheitsprobleme in der Vergangenheit, Bsp.

- ROBOT
- BEAST
- POODLE
- Heartbleed
- RC4 Biases
- CRIME
- BREACH
- ...

Quelle / Weitere Infos: https://github.com/hannob/tls-what-can-go-wrong

Gegenmaßnahmen

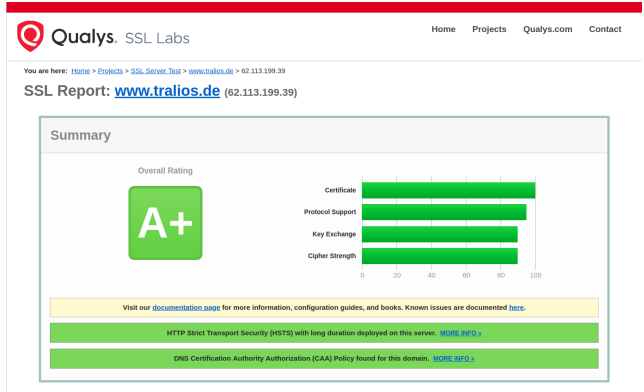
TRALIOS
Linux Server Management

- Software aktuell halten!
- Anfällige Protokolle & Cipher ausschalten, Beispiel Apache:

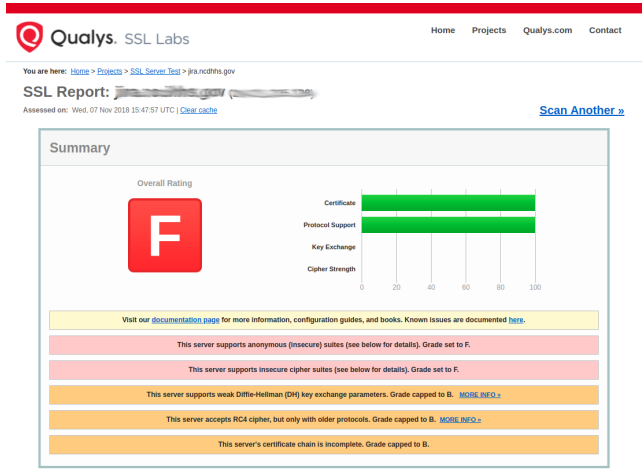
```
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:
ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:
ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:
ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:
DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:
DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:!ECDHE-RSA-RC4-SHA:!ECDHE-ECDSA-RC4-SHA:
AES128:AES256:!RC4-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!3DES:!MD5:!PSK
```

- Kontrolle, Bsp. Qualys SSL Labs Test: https://www.ssllabs.com/ssltest/

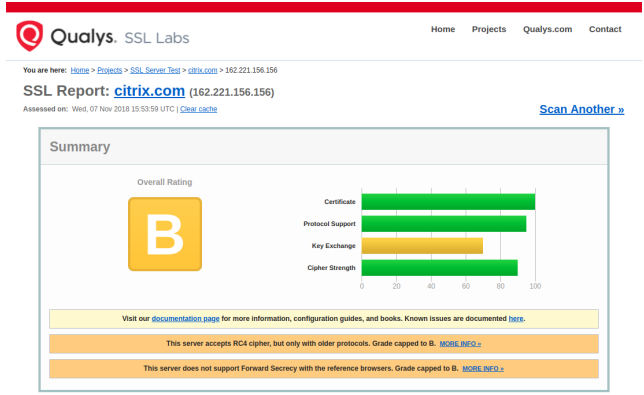
Beispiel: Domain mit Qualys A+ Bewertung



Negativbeispiel: Domain mit Qualys F Bewertung



Domain mit Qualys B Bewertung



Wahrscheinlich Absicht aufgrund von Kompatibilitätseinschränkungen

Fazit

TRALIOS
Linux Server Management

- Zahlreiche Unterschiede zwischen den Zertifikate
- Neue Einflüsse durch Let’s Encrypt
- SSL ist inzwischen Standard
- Umsetzung wichtig, zahlreiche Randeffekte zu beachten

Weitere Themen / Diskussion

TRALIOS
Linux Server Management

- **Revokation**: Zurückziehen von kompromittierten Zertifikaten
- **HTTP Strict Transport Security (HSTS)**: Erzwingen von SSL
- **HTTP Public Key Pinning (HPKP)**: Längere Festlegung auf bestimmte Zertifikate
- **Certificate Transparancy**: Veröffentlichung von ausgestellten Zertifikaten
- **DNS CAA**: Berechtigung zur Ausstellung von Zertifikaten festlegen
- **Server Name Indication (SNI)**: Erweiterung zur Nutzung mehrerer Domains

Kontakt

TRALIOS
Linux Server Management

- Dipl.-Inform. Dominik Vallendor

- Tralios IT GmbH
  Douglasstr. 24-26
  76133 Karlsruhe
  Telefon: 0721 - 94269660
  Telefax: 0721 - 94269666
  E-Mail: vallendor@tralios.de