SSL/TLS Server-Zertifikate

BB-ONE net
Internet-Partner der Wirtschaft

Vitamine für Ihr Business


Secure
https://

BB-ONE net

Agenda

- Begriffs-Bestimmung
- Wofür sind TLS-Server-Zertifikate gut?
- Umstellung(en) planen!
- Nach Umstellung: Prüfen

BB-ONE net

Was ist ein TLS-Server-Zertifikat?

- Zertifikate sind Textdateien
- Es besteht aus einer oder zwei Dateien:
  - www.bb-one.net.crt: das eigentliche Zertifikat
  - www.bb-one.net.ca-bundle: ein Zwischen-Zertifikat
- Zusätzlich kommt der „Server-Key“ zum Einsatz

BB-ONE net

Ein Zertifikat

```
-----BEGIN CERTIFICATE-----
MIIFJjCCBA6gAwIBAgIRAKF5eursS1TPHJDN0mksQgwwDQYJKoZIhvcNAQEFBQAw
czELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4G
A1UEBxMHU2FsZm9yZDEaMBgGA1UEChMRQ09NT0RPIENBIExpbWl0ZWQxGTAXBgNV
BAMTEFBvc2l0aXZlU1NMIENBIDIwHhcNMTQwNDI1MDAwMDAwWhcNMTcwNDI0MjM1
OTU5WjBfMSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0ZWQxFDASBgNV
BAsTC1Bvc2l0aXZlU1NMMSQwIgYDVQQDExtkcm9waW4uY2xvdWRzZXJ2aWNlcy5i
ZXJsaW4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDcBXZxZzKe0wzc
cdKcXrVBypTNtLDDCDusji/NTbAg02zgQGkX4cmADDZ0R43ttLB4i0gtASX2l962
PRj8ny8icYHYc0IpqQR2S7esej0Ur+GXywXgET1puTygicBjTkw/0LHtaAcpyart
VRpJcaYDr72iAhN9AUWI6dzeBoEqXlkNFKgYdfNfDDfBdDz4wuD3QScplp8Wrnzj
jxg0h2c6KrOA2XiO1b1HGuycx4BqsHNNh3Bn/lIqYg4raNtqMWqDTVIHdOnlL5sU
+fLhQCQidbVeYGCxGBT2PFVUbbowEWJevuP/Vwgw1Pig6roTIl5Vnlr/RIppKgDE
3Wgo0pyBAgMBAAGjggHHMIIBwzAfBgNVHSMEGDAWgBSZ5EBfaxRePgXZ3dNjVPxi
uPcArDAdBgNVHQ4EFgQUXzknGEDR4IZNvxlNeAEeCNtP+ikwDgYDVR0PAQH/BAQD
AgWgMAwGA1UdEwEB/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MFAGA1UdIARJMEcwOwYLKwYBBAGyMQECAgcwLDAqBggrBgEFBQcCARYeaHR0cDov
L3d3dy5wb3NpdGl2ZXNzbC5jb20vQ1BTMAgGBmeBDAECATA7BgNVHR8ENDAyMDCg
LqAshipodHRwOi8vY3JsLmNvbW9kb2NhLmNvbS9Qb3NpdGl2ZVNTTENBMi5jcmww
bAYIKwYBBQUHAQEEYDBeMDYGCCsGAQUFBzAChipodHRwOi8vY3J0LmNvbW9kb2Nh
LmNvbS9Qb3NpdGl2ZVNTTENBMi5jcnQwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3Nw
LmNvbW9kb2NhLmNvbTBHBgNVHREEQDA+ghtkcm9waW4uY2xvdWRzZXJ2aWNlcy5i
ZXJsaW6CH3d3dy5kcm9waW4uY2xvdWRzZXJ2aWNlcy5iZXJsaW4wDQYJKoZIhvcN
AQEFBQADggEBAGpLLDpkuvzME+LNZD+nNJkMyTZ/0QTq/ppMgvcVveciydutEcSA
+GfaYYknXNYkQX1igoRi40H1Se60Llgpo1To4FIe3032cU9H2YdHpBpaAq6G8qdC
u8qZ7OPdnHTNjilgtWI86uqUp7VbjuMVtsUdUCMWeg5TAIO0+dsVHdLAbbV9p918
Bk0ZIRAltQmHZbXj/76MdCB08nh1wIqs5rbegBIdMmYTtLK+WMlqyDzNWirRCCYm
D9ecpNJE8d7a066C5Jk2aZQS/0i9FUjnYtw4SYf9mgZRTo1MI1IhymcmsYaZsehx
hLWpX2EQCavY+twZLDp+wuppZ1fdSTeY3+U=
-----END CERTIFICATE-----
```

BB-ONE net

Wo kommt das Zertifikat her?

- Auf dem Server wird ein Certificate Request erstellt …
- … und an eine Certificate Authority gesandt
- Certificate Authority gibt nach Prüfung das Zertifikat aus

BB-ONE net

Zertifikats-Unterschiede

- Überprüft wird …
- … die Domain oder …
- … die Organisation / die Person.
- Achtung: Wildwuchs!
- Grosse Namen schützen nicht vor „Fehlern“

Certificate Authority oder Trust Center

Ein TrustCenter soll eine **vertrauenswürdige dritte Instanz** (Trusted Third Party) darstellen,
welche in elektronischen Kommunikationsprozessen die jeweilige **Identität des Kommunikationspartners** bescheinigt.

Beispielsweise übernehmen Zertifizierungsdiensteanbieter (Certification Authority) in der elektronischen Kommunikation im Zusammenhang mit elektronischen Signaturen die Rolle eines TrustCenters, welches Zertifikate ausstellt,
anhand derer die Identität des Kommunikationspartners bescheinigt werden soll.

Wikipedia

BB-ONE net

Wo kommt das Zertifikat hin?

- Zertifikat wird in die Konfiguration des Webservers eingetragen

Beispiel für Apache

```
<VirtualHost *:443>
    ...
    SSLEngine on
    SSLCertificateFile      /home/cert/www.bb-one.net.crt
    SSLCertificateChainFile /home/cert/www.bb-one.net.ca-bundle
    SSLCertificateKeyFile   /home/cert/www.bb-one.net.key

    # Konfiguration für HSTS
    Header always set Strict-Transport-Security "max-age=15768000"
    ...
    # SSL-Konfiguration
    ...
</VirtualHost>
```

BB-ONE net

Wo nutzt ein Zertifikat?

- Verschlüsselung
- Reputation
- Ranking-Kriterium bei Suchmaschinen
- HTTP/2

BB-ONE net

Verschlüsselung

- Verschlüsselt wird:
  - Datenverkehr zwischen Webserver und Browser
  - Mail-Formulare
  - Shops
  - ...

BB-ONE net

Reputation

- Browser bewerten HTTPS positiv bzw. …
- … das Fehlen oder eine Implementierung negativ
- Warn-Hinweise á la „Rauchen tötet“

BB-ONE net

Firefox

Diese Verbindung ist nicht sicher

Der Inhaber von www. [redacted] .de hat die Website nicht richtig konfiguriert. Firefox hat keine Verbindung mit dieser Website aufgebaut, um Ihre Informationen vor Diebstahl zu schützen.

Weitere Informationen...

☐ Fehler an Mozilla melden, um beim Identifizieren und Blockieren böswilliger Websites zu helfen

Zurück | Erweitert

BB-ONE net

IE

Es besteht ein Problem mit dem Sicherheitszertifikat der Website.

Das Sicherheitszertifikat dieser Website wurde für eine andere Adresse der Website ausgestellt.

Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten die Sie an den Server gesendet haben abzufangen.

Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.

Klicken Sie hier, um diese Webseite zu schließen.

Laden dieser Website fortsetzen (nicht empfohlen).

Weitere Informationen

BB-ONE net

Chrome

Dies ist keine sichere Verbindung

Hacker könnten versuchen, Ihre Daten von **www.[redacted]de** zu stehen, zum Beispiel Passwörter, Nachrichten oder Kreditkartendaten. Weitere Informationen

NET::ERR_CERT_COMMON_NAME_INVALID

☐ Ich möchte automatisch einige Systeminformationen und Seiteninhalte an Google senden, um bei der Erfassung schädlicher Apps und Websites zu helfen. Datenschutzerklärung

ERWEITERT

Zurück zu sicherer Website

BB-ONE net

Ranking

- Google 2014: HTTPS ist ein Ranking-Faktor
- Bei Brand-Sites waren bis
  5 % mehr Traffic zu beobachten
- Ohne HTTPS = Ranking-Nachteil

BB-ONE net

HTTP/2

- „Neues“ Protokoll (seit 2014!)
- Beschleunigt die Datenübertragung deutlich

- Ab Apache 2.4.12 und NGINX 1.9.5

- **Browser unterstützen HTTP/2 nur mit HTTPS**

BB-ONE net

Umsetzung planen

- Zertifikat erwerben
- Server-Konfiguration
- Verlinkung
- Prüfen
  - Logfiles
  - Website-Analyzer

BB-ONE net

Webinar HTTPS-Umstellung

BB-ONE net

Die Inhalte

- Praxis-Beispiel: kleine WebSite mit WordPress
- Zertifikat erwerben
- Vorbereitungen auf dem Server
- Umstellungen im CMS
- Nachbereitungen (was wurde vergessen)

BB-ONE net
Internet-Partner der Wirtschaft

Internetpartner der Wirtschaft

Vitamine für Ihr Business