HTTPS & SSL/TLS Server-Zertifikate

BB-ONE net
Internet-Partner der Wirtschaft

Vitamine für Ihr Business


Secure
https://

BB-ONE net

Agenda

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

Chrome markiert bald alle HTTP-Webseiten als unsicher

09.02.2018 10:25 Uhr – Daniel Berger

vorlesen

Ab Juli wird der Chrome-Browser alle unverschlüsselten HTTP-Webseiten deutlich als unsicher kennzeichnen. Googles Botschaft an Seitenbetreiber: Setzt endlich HTTPS ein!

BB-ONE net

Bisher?

- Chrome warnt bei Formularen ohne HTTPS

BB-ONE net

Und Firefox?

www.brak.de/service/kontakt/

Suchen

Seiteninformationen anzeigen

www.brak.de

Verbindung ist nicht sicher

Schutz vor Aktivitätenverfolgung

Keine Inhalte zur Aktivitätenverfolgung auf dieser Seite gefunden.

Berechtigungen

Der Website wurden keine besonderen Berechtigungen erteilt.

Herr Firma

234567

main.de

Adresse*

Ihre Mitteilung

Betreff* Betreff

Mitteilung* Mitteilung

BB-ONE net

Und nun?

- Handlungsbedarf:
  - Webserver-Software aktualisieren
  - Qualifiziertes Zertifikat erwerben
  - Korrekt implementieren
  - Website auf HTTP-Referenzierungen überprüfen
  - HSTS aktivieren
  - HTTP/2 aktivieren

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
PRj8nyi8cYHYc0IpqQR2S7esej0Ur+GXywXgET1puTygicBjTkw/0LHtaAcpyart
VRpJcaYDr72iAhN9AUWV6dzeBoEqXlkNFKgYdfNfDDfBdDz4wuD3QScpl p8WvnzJ
jxg0h2c6KrOA2Xi O1b1HGuycx4BqsHNNh3Bn/lIqYg4raNtqMWqDTVI HdOnl L5sU
+fLhQCQidbVeYGCxGBT2PFVUbbowEWJevuP/Vwgw1Pig6roTIl 5Vnlr/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+WMiqyDzNWirRCCYm
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

Zertifizierung: Google entzieht Symantec 2018 das Vertrauen UPDATE

13.09.2017 09:10 Uhr – Jürgen Schmidt

vorlesen

www.heise.de

Ab April wird der Google-Browser Chrome für Zertifikate Fehler melden, die Symatecs CAs ausgestellt haben. Dazu gehören unter anderem Thawte, VeriSign, Equifax, GeoTrust und RapidSSL. Wer die noch im Einsatz hat, muss bald handeln.

SSL Report: bb-one.net (193.193.167.15)

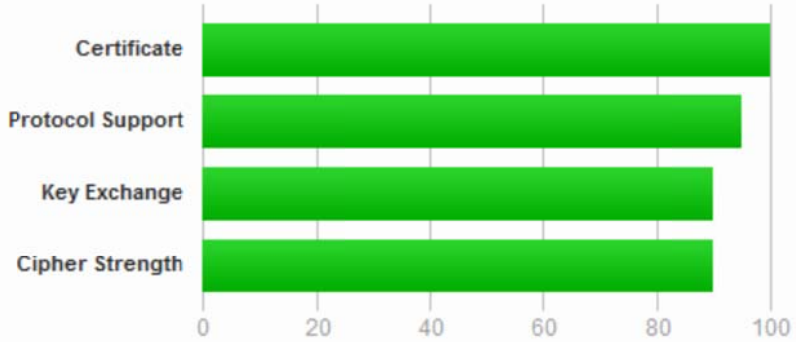
Assessed on: Thu, 15 Feb 2018 08:28:01 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

SSL Report: anwaltverein.de (78.46.140.196)

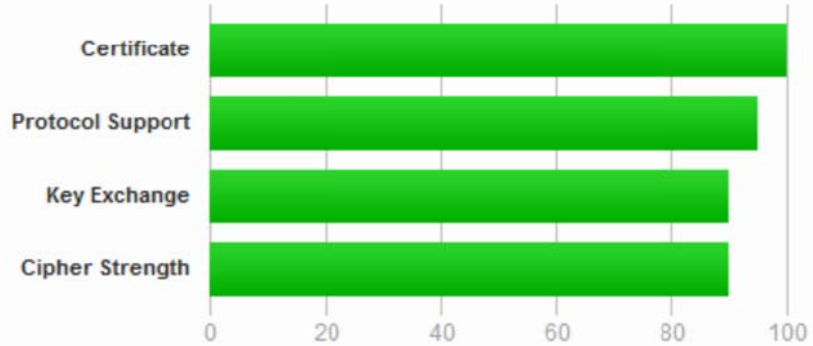
Assessed on: Thu, 15 Feb 2018 08:34:53 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate will be distrusted by Google and Mozilla from March 2018. MORE INFO »

SSL Report: brak.de (85.10.199.234)

Assessed on: Thu, 15 Feb 2018 08:56:30 UTC | Hide | Clear cache

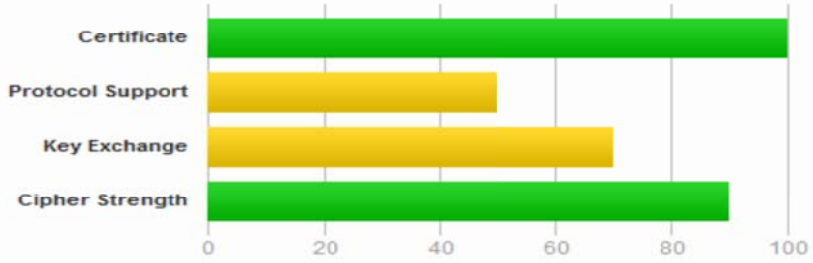
Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

This server does not support Forward Secrecy with the reference browsers. Grade will be capped to B from March 2018. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade will be capped to B from March 2018. MORE INFO »

This server's certificate will be distrusted by Google and Mozilla from September 2018. MORE INFO »

BB-ONE net

SSL-Check

- SSL-Check mit Bewertung:
  - Email an ssl-check@bb-one.net
  - zu prüfende URL
  - muss im eigenen Besitz sein

BB-ONE net

Wo kommt das Zertifikat hin?

- In die Konfiguration des Webservers:

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

    Header always set Strict-Transport-Security "max-age=15768000"

</VirtualHost>
```

BB-ONE net

- In die Konfiguration des Webservers:

Beispiel für NGINX

```
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;

    ssl_certificate /home/cert/www.bb-one.net.crt; (inclusive bundle!)
    ssl_certificate_key /home/cert/www.bb-one.net.key;

add_header Strict-Transport-Security max-age=15768000;

}
```

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.** **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

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

Need help?

- Implementierungs-Service:
- ssl-implementierung@bb-one.net

Vitamine für Ihr Business