IT-Sicherheit in der Praxis

25. Deutscher EDV-Gerichtstag 2016
Saarbrücken

Dr. Ronald Petrlic

- Aufgaben und Arbeitsschwerpunkte
  - Kontrolliert Einhaltung des Datenschutzes durch verantwortliche Stellen
  - Bearbeitung von Eingaben von Bürgerinnen und Bürgern
  - Stellungnahmen zu Gesetzentwürfen und Projekten
  - Beratung von DS-Beauftragten, Behörden und Unternehmen
  - **Automatisierte, groß angelegte Prüftätigkeiten (im technischen Bereich)**
- Befugnisse
  - Zutritt zu Dienst- bzw. Geschäftsräumen, Vornahme von Prüfungen und Besichtigungen
  - Einsichtnahme in geschäftliche Unterlagen, gespeicherte Daten und DV-Programme
  - Gebührenpflichtige Anordnung der Mängelbeseitigung

Unsere Ziele

- Aktuelles Projekt: Datenschutzrechtliche Überprüfung von Internetauftritten
  - Das (technische) Datenschutzniveau von Webseiten mittelständischer Unternehmen in Baden-Württemberg soll verbessert werden
  - Teilprojekt: Überprüfung des Einsatzes einer sicheren Verschlüsselung
    - Die IT-Sicherheit von Webseiten mittelständischer Unternehmen in Baden-Württemberg soll verbessert werden

Unsere Vorgehensweise

Status: beendet

Status: in Arbeit

Status: in Planung

Rechtliche Grundlage

§ 13 Telemediengesetz – Pflichten des Diensteanbieters

(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und

2. diese

a) gegen Verletzungen des Schutzes personenbezogener Daten und

b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind.

Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Rechtliche Grundlage

§ 16 Telemediengesetz – Bußgeldvorschriften

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

…

3. einer Vorschrift des § 13 Abs. […] Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a

über eine dort genannte Pflicht zur Sicherstellung zuwiderhandelt,

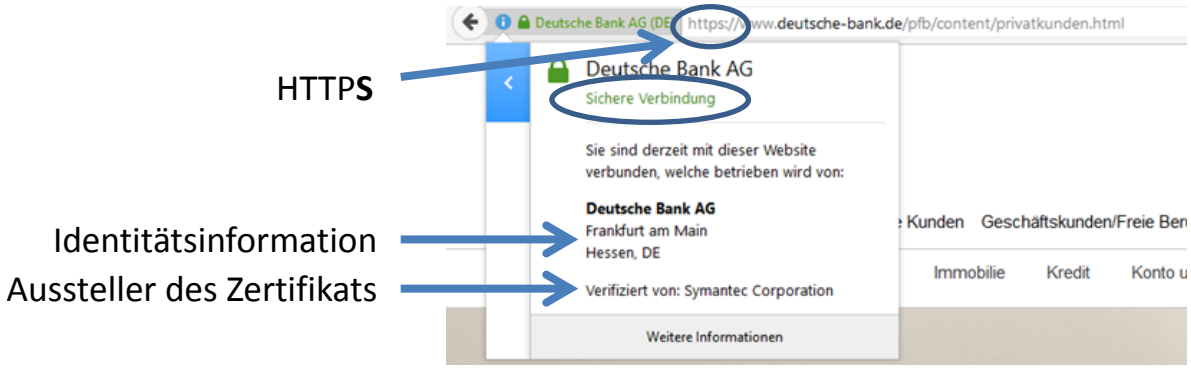
…

(3) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

Technische Grundlage

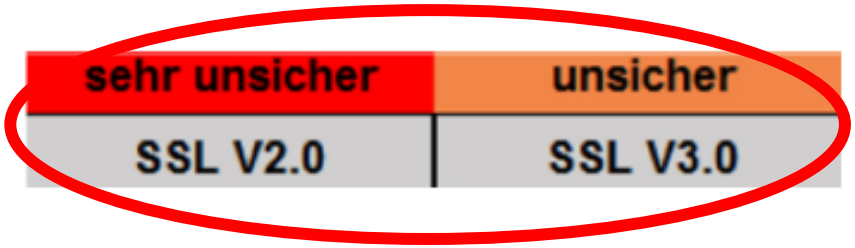
- TLS (Transport Layer Security) als **das** Sicherheitsprotokoll im Internet
  - Auch bekannt unter der früheren Bezeichnung „Secure Sockets Layer“ (SSL)
  - Nicht nur Verschlüsselungsverfahren (für Vertraulichkeit der Daten), sondern bietet zusätzlich Integrität und Authentizität der übertragenen Daten

    → garantiert, dass Betrüger etwa Kommunikation im Web (bspw. beim Online-Banking) nicht mitlesen, nicht verändern können, etc.

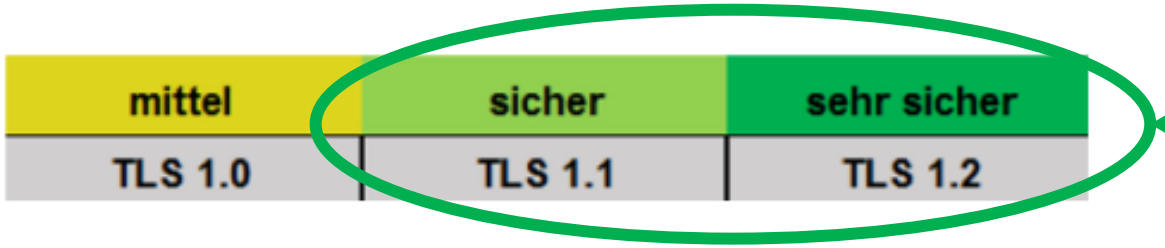


Technische Grundlage

- Qualität der SSL/TLS-Protokollversionen



Nicht mehr sicher nach dem Stand der Technik



BSI-Vorgaben!

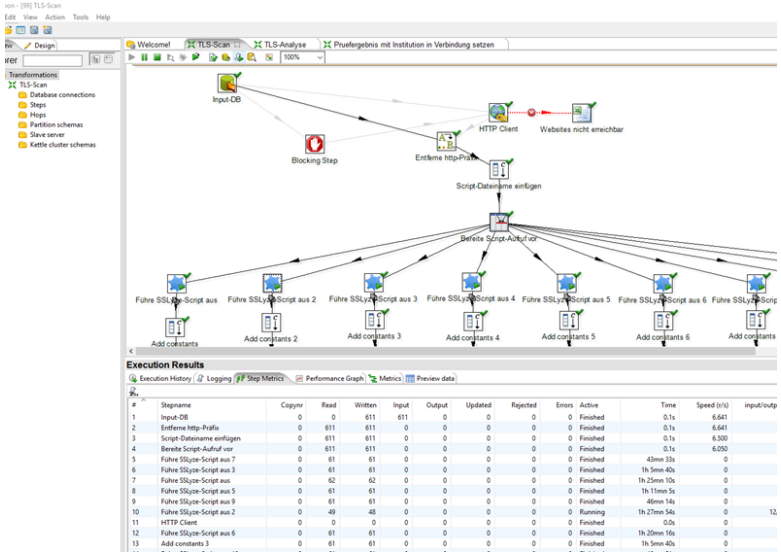
Als Übergangs-lösung noch in Ordnung

Sicher nach dem Stand der Technik

Quelle: Pohlmann, https://www.stuttgart.ihk24.de/blob/sihk24/Fuer-Unternehmen/innovation/downloads/3300070/801b0ef29405c1710223f9a76bc24c06/TLS-Check-Ergebnisse-data.pdf

Technische Prüfplattform

- Eigene Entwicklung einer Prüfplattform, basierend auf Business Intelligence-Werkzeug
  - Komplexe Prüftätigkeiten „einfach“ durchführbar (auch durch Nicht-Techniker)
  - Modularer Ansatz → können rasch weitere Prüfkriterien mit einbeziehen
  - Verwendung gängiger Werkzeuge (SSLyze, Nmap, etc.)
  - Qualitätskontrolle durch stichprobenartige Prüfung (händisch und mittels weiterer Tools)



Durchführung der Prüfung

- Datenbasis: 39.633 URLs von Internetauftritten Baden-Württembergischer Unternehmen
  - davon 3.339 nicht erreichbar
- Mehrere Prüfungen durchgeführt
  - 1. Prüfung: März 2016
  - 2. Prüfung: Juni 2016
  - 3. Prüfung: September 2016
- Prüfzeit: ca. 40 Stunden (mit einem Rechner)

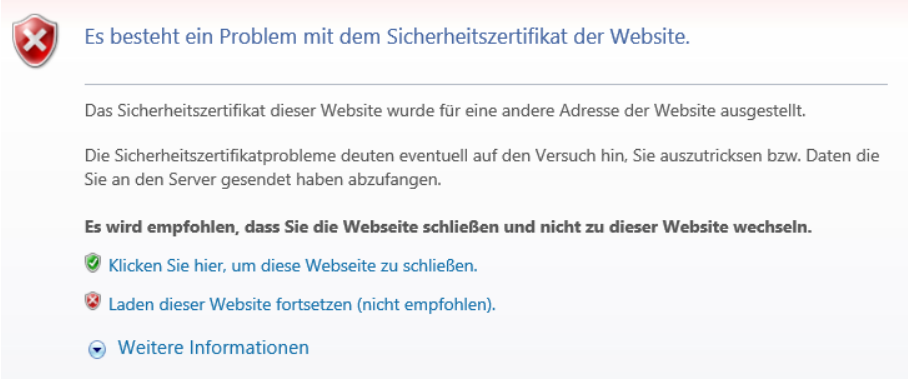
Ergebnis

- 10.330 bereitstellende Webserver bieten HTTPS (über SSL/TLS) an

  → **28 %**

  - ABER: „Certificate Hostname Mismatch“ in ¾ dieser Fälle!
    - D.h. Eindeutige Bezeichnung des Rechners im Internet stimmt nicht mit hinterlegtem Namen im Zertifikat überein

    → potentiell Gefahr eines Man-in-the-middle-Angriffs
      - Angreifer gibt sich als legitimer Webserver aus



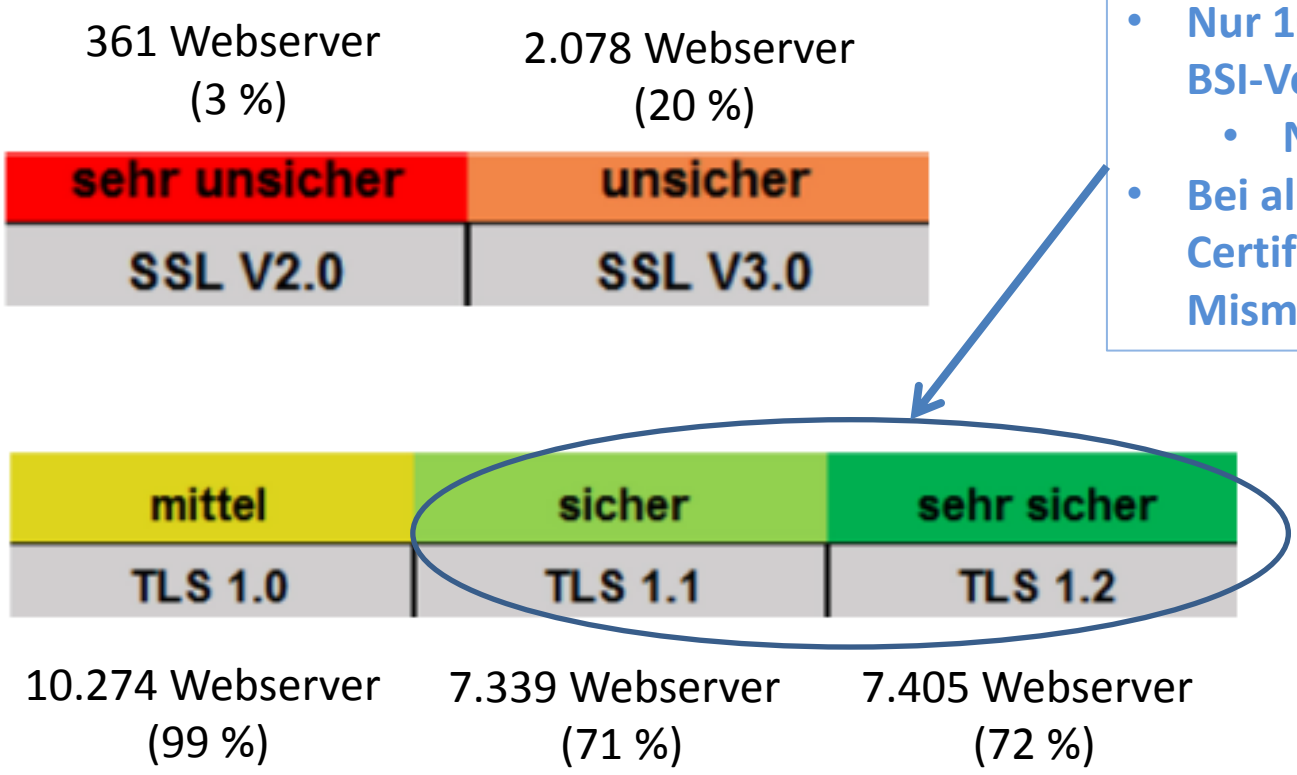
Ergebnis

- Unsere Untersuchungen haben gezeigt, dass in den meisten Fällen wahrscheinlich kein Angriff vorliegt
  - Grund für hohe Zahl an „falschen“ HTTPS-Angeboten:
    - Webseiten werden von großen Hosting-Anbietern ausgeliefert, die lediglich andere (als die geprüften) Webseiten über HTTPS anbieten
    - „Common Name“ im Zertifikat enthält nicht Domain der Webseite sondern erfasst nur speziellen Bereich (bspw. „shop.example.com“ → Sichere Verbindung erst beim „Betreten“ des Online-Shops)

- **Tatsächliches Angebot von Webseiten über HTTPS also zwischen 7 % und 28 % (eher im unteren Bereich)**

Ergebnis

- Unterstützte SSL/TLS-Versionen



- **Nur 10! Webserver halten BSI-Vorgaben ein**
  - **NUR TLS ab Version 1.1**
- **Bei allen 10 Fällen gibt es Certificate Hostname Mismatch**

Ergebnis

- Weitere Erkenntnisse
  - 45 Webserver (0,4 %) nach wie vor von Heartbleed-Bug betroffen
  - 83 % aller untersuchten Zertifikate konnten mit dem Google Zertifikatspeicher erfolgreich validiert werden (spricht ebenfalls gegen MITM-Angriffe)
  - 86 % der Zertifikate haben eine RSA-„Public Key Size“ von 2048 Bit (sicher nach dem Stand der Technik)

- Unterstützung neuartiger Ansätze (noch nicht Stand der Technik)
  - 8 % unterstützen HTTP Strict Transport Security (HSTS)
  - 4 % unterstützen OCSP Stapling
  - 16 Webserver unterstützen HTTP Public Key Pinning (HPKP)

Fazit und Ausblick

- Größte derartige Prüfung mit „richtigen“ Unternehmens-Webseiten
- Bisher eher mangelhafte Umsetzung der Vorgaben zur IT-Sicherheit bei Unternehmen in Baden-Württemberg
  - Als nächstes werden Behörden-Webseiten geprüft
- Aufklärungsarbeit nötig (Pressemitteilungen, Vorträge, Leitfäden zur Umsetzung der Vorgaben, etc.)
  - Beobachten, inwieweit Ansätze wie „Let‘s Encrypt“ und Vorstoß von Amazon für kostenlose Zertifikate eine Verbesserung bringen
  - Verbessertes Ranking bei Google durch Einsatz von HTTPS könnte Situation ebenfalls verbessern
- Geplant sind regelmäßige Wiederholungsprüfungen
- Weitere Prüfungen zur technischen Umsetzung von Datenschutzvorgaben
- Personalisierte Ansprachen bzw. Anordnungen ebenfalls möglich

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Ronald Petrlic
Beim Landesbeauftragten für den Datenschutz Baden-Württemberg
Königstraße 10a
70173 Stuttgart
petrlic@lfd.bwl.de
www.baden-wuerttemberg.datenschutz.de