SSL-Zertifikate

Dr. Christopher Kunz

Ihr Referent

filoo®
member of Thomas Krenn Group

- Dr. Christopher Kunz
- CEO Hosting filoo GmbH / TK AG
- Promotion IT Security
  - X.509 / SSL
- Vorträge auf Konferenzen
  - OSDC 2012: SSL-Hacks
  - OSDC 2014: Heartbleed
- Artikel in Fachmagazinen, Fachbücher

Filoo GmbH

member of Thomas Krenn Group

- Wir sind die Hosting-Tochter der Thomas-Krenn.AG
  - Sicheres, hochperformantes Hosting in Frankfurt
  - Mitarbeiter in Gütersloh und Freyung
- Eigene Public Cloud
  - Open-Source Cloud Middleware
  - VMWare Cloud
- Managed Services
  - Security Services
  - Systemadministration
  - Planung & Deployment

Agenda

member of Thomas Krenn Group

- Was ist SSL und wofür ist es gut?
- SSL-Zertifikate erklärt
- Einsatzmöglichkeiten
- SSL und Google
- SSL-Produkte bei filoo / Thomas-Krenn
- Fragen / Antworten

SSL – was ist das?

filoo®
member of Thomas Krenn Group

- SSL bedeutet „Secure Sockets Layer“ („Schicht für sichere Anschlüsse“)
- Protokollsammlung für die Verschlüsselung von Datenübertragung
  - Nicht für die Verschlüsselung von Dokumenten/Dateien
- Aktuelle Version 3.0 (seit 1995!)
- Erfüllt viele Aufgaben
  - Vertraulichkeit
  - Integrität
  - Authentizität

TLS vs. SSL

filoo®
member of Thomas Krenn Group

- TLS ist „SSL, Next Generation“
- Aktuelle Version 1.2 (von 2008)
  - Noch nicht überall unterstützt
- Wird in vielen Produkten verwendet
  - Webserver
  - Mailserver
  - Instant Messaging
  - U.v.m.
- Oft sagen wir „SSL“, meinen aber „TLS“

SSL als Verschlüsselung

filoo®
member of Thomas Krenn Group

- SSL ist sogenannte „Transportverschlüsselung“
  - Daten werden für den Transport verschlüsselt
  - Wichtig: Hohe Geschwindigkeit (=Durchsatz)
  - Früher nicht so wichtig: Aufwendige Verschlüsselung

- SSL ist nicht für die permanente Verschlüsselung
  - ...z.b. Kundendaten in der Datenbank
  - Dafür gibt es z.B. GPG und Crypto-Container

SSL zur Identifikation

filoo®
member of Thomas Krenn Group

- Digitale Zertifikate
  - „Elektronischer Ausweis“ bestehend aus Krypto-Schlüsseln
  - Identifikation z.b. über Name, E-Mail, Domainname
- Zertifikate werden beim Aufbau einer SSL-Verbindung „vorgezeigt“
  - ...also z.b. beim Aufruf von https://meinshop.de/
- Antwort auf die Frage: „rede ich wirklich mit meinshop.de?“

Was bringt das jetzt?

filoo®
member of Thomas Krenn Group

- Abhörsicherheit
  - Daten sind verschlüsselt
  - Abhören zwar möglich, Entschlüsseln aber nicht
  - Abgreifen von pers. Daten, Passwörtern extrem erschwert
- Identifikation
  - Nutzer sehen, mit wem sie sprechen
  - Angreifer können sich nicht zwischenschalten
- Manipulationssicherheit
  - Daten können nicht auf dem Weg manipuliert werden
  - Bestellmengen ändern, Trojaner in Mails einfügen etc.

Ein SSL-Zertifikat

filoo®
member of Thomas Krenn Group

-----BEGIN CERTIFICATE-----

MIIFJDCCBAygAwIBAgIDEjVeMA0GCSqGSIb3DQEBBQUAMDwxCzAJBgNVBAYTAlVT

MRcwFQYDVQQKEw5HZW9UcnVzdCwgSW5jLjEUMBIGA1UEAxMLUmFwaWRTU0wgQ0Ew

HhcNMTQwNDE1MjAzMDEwWhcNMTYwMjI5MTcwNTU2WjCBuTEpMCcGA1UEBRMgRDND

QjVZN08waUQvVm9hTzhZZjBHV0pxekstd0JEVHAxEzARBgNVBAsTCkdUMjY2NDE1

ODYxMTAvBgNVBAsTKFNlZSB3d3cucmFwaWRzc2wuY29tL3Jlc291cmNlcy9jcHMg

KGMpMTQxLzAtBgNVBAsTJkRvbWFpbiBDb250cm9sIFZhbGlkYXRlZCAtIFJhcGlk

U1NMKFIpMRMwEQYDVQQDDAoqLmZpbG9vLmRlMIIBIjANBgkqhkiG9w0BAQEFAAOC

AQ8AMIIBCgKCAQEAlMDDk5YCYM7Br6OZ2pfLvnIkIDtsk/aHmQ9lBqCbRTJeyUok

[...]

zdzISbQlVsM103aIN7Rpz6AEsLse2v/TBKnjIQTHI3aM4WJE952QzBQrVwOMPjk9

x1CtD2rI6cxCYEUZxiI4QYMC1/b/Iifj5OkLAFyuDGwqMxpq0w2kqA2Hz0kaKmjM

-----END CERTIFICATE-----

SSL-Zertifikat Klartext

member of Thomas Krenn Group

```
Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=GeoTrust, Inc., CN=RapidSSL CA
        Validity
            Not Before: Apr 15 20:30:10 2014 GMT
            Not After : Feb 29 17:05:56 2016 GMT
        Subject: serialNumber=D3CB5Y7O0iD/VoaO8Yf0GWJqzK-
wBDTp, OU=GT26641586, OU=See
www.rapidssl.com/resources/cps (c)14, OU=Domain Control
Validated - RapidSSL(R), CN=*.filoo.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Vertrauen ist gut…

filoo®
member of Thomas Krenn Group

- …Kontrolle ist besser!
- Wie stelle ich Vertrauen her?
- Im richtigen Leben: Vertrauenswürdige Behörde
  - Notar, Ausweisstelle, etc.
- Im Internet: Zertifikatsaussteller (CA)
  - Vertrauenswürdig durch aufwändige Prüfungen
  - In Browsern fest integriert
- Auch hier gibt es schwarze Schafe!

Was sind CAs?

filoo®
member of Thomas Krenn Group

- Certificate Authority
  - „Zertifikats-Autorität“
- Organisation oder Firma, die Zertifikate ausstellt
  - Kann eigentlich jeder
- „Vertrauenswürdige CA“ kann nicht jeder sein
  - Langer Zertifizierungsprozeß
  - Mehrere Hundert vertrauenswürdige CAs
- Vertrauen wird in SSL-Komponenten verankert
  - Betriebssysteme, Browser, Mailclients, Server

Ohne Vertrauen

filoo®
member of Thomas Krenn Group

Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu **www.solwatch.eu** aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

Diese Seite verlassen

▸ **Technische Details**

▸ **Ich kenne das Risiko**

Mit Vertrauen

filoo®
member of Thomas Krenn Group

SSL und Google

filoo®
member of Thomas Krenn Group

- Google fordert seit Jahren mehr Verschlüsselung
- Ankündigung am 6. August: HTTPS als Rankingfaktor
- https://domain.de rankt besser als http://domain.de
- Momentan noch geringe Auswirkungen
  - „Over time, we might decide to strengthen it“
  - „Im Laufe der Zeit könnten wir [die Auswirkung] verstärken“
- Sie können Ihre Suchplazierung durch SSL (etwas) verbessern

SSL und Google

filoo®
member of Thomas Krenn Group

- Guter Zeitpunkt für „SSL Only“ auf Webseiten
  - Alle Seiten SSL-verschlüsselt ausliefern
  - Weiterleitung von http:// auf https://
  - Achtung vor doppelt plazierten Inhalten!
- U.U. mehrere Zertifikate notwendig
  - Images.ihredomain.de, static.ihredomain.de
- Achtung bei Trackern/Analytics-Tools
  - Diese müssen SSL unterstützen

Was heißt das für mich?

member of Thomas Krenn Group

- Ihr Webserver braucht SSL
  - Verschlüsselung von Bestellungen
  - Abhörsicherheit / Vertraulichkeit
- Sie benötigen ein Zertifikat
  - Nach Ihren Bedürfnissen
  - Mit ausreichender Sicherheit
  - Für alle genutzten Domains und Dienste
- Das Zertifikat muss vertrauenswürdig sein
  - Eine kommerzielle CA muss es ausstellen

Zertifikats-Arten

filoo®
member of Thomas Krenn Group

- Single-Domain-Zertifikat
  - Gültig nur für www.ihredomain.de
- Wildcard-Zertifikat
  - Gültig für *.ihredomain.de
  - Meist auch für ihredomain.de
- Extended-Validation-Zertifikat
  - Gültig nur für www.ihredomain.de
  - Besonders gründliche Prüfung

SSL123 Zertifikat

filoo®
member of Thomas Krenn Group

- Zertifikat für einen Domainnamen
  - Etwa: www.ihredomain.de
- Gültigkeit 1,2 oder 3 Jahre
  - i.d.R. am selben Werktag ausgestellt
- Prüfung über die Domain
  - Verifizierungs-E-Mail
- Kompatibel mit allen Browsern + Smartphones

Wildcard-Zertifikat

filoo®
member of Thomas Krenn Group

- Zertifikat für viele Subdomainnamen
  - www.ihredomain.de, static.ihredomain.de, mail.ihredomain.de etc.
  - Ihredomain.de
  - Nicht 1.mail.ihredomain.de etc.
- Gültigkeit 1,2 oder 3 Jahre
  - Ausstellung i.d.R. am selben Werktag
- Prüfung über die Domain
  - Verifizierungs-E-Mail

Extended Validation

filoo®
member of Thomas Krenn Group

- Hohe Sicherheit

- Zertifikat für eine Subdomain
  - www.ihredomain.de
  - Keine Wildcard-Zertifikate möglich
- Hoher Aufwand zur Ausstellung
  - Bestätigungs-Mail, Firmen-Dokumentation, Rückruf
  - Dauer bis Ausstellung i.d.R. 3-10 Werktage

Wie bestelle ich?

member of Thomas Krenn Group

- Produkt und Laufzeit auswählen
- Zertifikats-Antrag erstellen („CSR“)
  - Technischer Vorgang, muss von Ihrem Administrator ausgeführt werden
  - Wir können helfen – fragen Sie unseren Vertrieb
- E-Mail-Adresse für Zertifikats-Bewilligung
  - admin, administrator, hostmaster, webmaster, postmaster @ihredomain.de
- Dokumentation vorbereiten
  - Notwendig nur für EV-Zertifikate

Beratung und Bestellung

filoo®
member of Thomas Krenn Group

- SSL123 und Wildcard direkt bestellen
  - <https://www.filoo.de/ssl-zertifikate.html>
  - Zertifikats-Wizard
- Unser Vertrieb hilft Ihnen gerne!
  - Rufen Sie uns unter 08551/9150-274 an
  - Schreiben Sie uns eine Mail unter <info@filoo.de>
- Weitere Fragen gern nach dem Webinar