



Nützliches zum Thema SSL-Zertifikate

Neuerung des TMG

Informieren Sie sich über das neue „IT-Sicherheitsgesetz“ und die Auswirkungen auf Ihr Geschäft.

Let's Encrypt

Seit Ende 2015 gibt es eine neue Möglichkeit der Verschlüsselung von

Tipps & Tricks

Wir verraten Ihnen die Besonderheit eines COMODO DV-Zertifikats und wie Sie Ihren Bestellprozess mit einer kleinen Änderung vielleicht noch besser machen können.



Sehr geehrte Kunden,

wir haben in diesem Newsletter einige für Sie **interessante** und vor allem **relevante Informationen** rund um das Thema **SSL-Zertifikate** zusammengestellt.

Neuerung des Telemediengesetzes (TMG):

Im Juni 2015 hat der Bundestag das „**Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme**“ verabschiedet. U.a. bringt dieses Gesetz auch **eine Änderung der Rechtslage für Anbieter von Telemedien, also z.B. für Onlineportale und Shops.**

Der neue § 13 Abs. 7 TMG lautet wie folgt:

(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.

Nachdem das Gesetz erst seit dem 1. August 2015, also gut einem halben Jahr, in Kraft ist, gibt es dazu noch keine Präzedenzfälle. Die Kommentatoren sind sich aber sehr einig, dass im Grunde **nur „nicht-kommerzielle Angebote“** von dieser Neuregelung **ausgenommen** sind.

SSL-Zertifikate bieten aufgrund ihrer weltweiten Akzeptanz als sichere Verschlüsselungstechnologie und – im Vergleich zu anderen Verfahren – dem sehr geringen

Installationsaufwand eine **optimale Möglichkeit**, den neuen Anforderungen gerecht zu werden. Wir empfehlen daher jedem Kunden, sein Angebot hinsichtlich des neuen TMG zu prüfen.

Sprechen Sie mit uns über Ihren Bedarf. Wir beraten Sie sehr gerne zu dem für Ihre Zwecke optimal geeignete Zertifikat und entwickeln mit Ihnen gemeinsam den optimalen Implementierungsprozess.

Let's Encrypt:

Im Zuge der Neuerung des TMG (s.o.) ist auch immer wieder von dem am Ende des vergangenen Jahres gestarteten Projekts „Let's Encrypt“ die Rede. Initiator ist eine gemeinnützige Gruppe amerikanischer IT-Unternehmen und Universitäten mit dem Ziel, die Verschlüsselung von Webinhalten zum allgemeinen Standard zu machen.

Wir haben die wichtigsten Fragen unserer Kunden zusammengefasst:

Was ist der Unterschied zw. z.B. Comodo und Let's Encrypt Zertifikaten?

Zunächst muss man hier unterscheiden und definieren. Es gibt verschiedene Vergabestellen (CAs) und verschiedene Cert-Klassen. CAs sind z. B. Comodo oder Thawte.

Klassen sind „dv“, also domainvalidiert oder „ov“ und „ev“ - also eine erweiterte Validierung inkl. sichtbaren Unternehmen im Zertifikat.

Let's Encrypt bildet dabei die Funktion der domainvalidierten Zertifikate ab. Es zielt also rein auf die Verschlüsselung der Datenverbindung ab.

Let's Encrypt kann - technisch gesehen - die domainvalidierten Einzelzertifikate ablösen. Es ist jedoch kein Ersatz für Wildcard- OV oder EV Zertifikate. OV und EV bringen die Funktion mit, den Zertifikatsinhaber (und somit Betreiber der WebSite) auszuweisen. Man kann ins Cert hineinschauen und sieht wer dahintersteckt.

Es ergeben sich weitere Fragen bzgl. der Markt-Akzeptanz und der Browser-Kompatibilität. Dazu muss man sich den Aufwand für eine Let's Encrypt Verschlüsselung ansehen. Momentan werden nur kurze Zeitabschnitte abgedeckt – ein dv-Zertifikat hat eine Laufzeit von bis zu drei Jahren. Diese Punkte können aus unserer Sicht momentan gegen den Einsatz von Let's Encrypt sprechen.

Warum sollte ich weiterhin Geld für Zertifikate ausgeben, wenn es diese auch kostenlos gibt?

Zum einen bieten die Zertifikate der traditionellen CAs selbst in der niedrigsten Klasse bereits eine Versicherungssumme von 10.000 USD. Sollte dem Website-Betreiber also aufgrund eines fehlerhaft ausgestellten Zertifikats ein Schaden entstehen, deckt die CA zumindest bis zu einem gewissen Betrag den entstandenen Schaden ab.

Zum anderen kaufen Sie mit den Zertifikaten nicht nur **state-of-the-art** Verschlüsselungstechnologie, sondern auch die damit verbundene **Dienstleistung**.

Die technisch sehr tiefe Integration insbesondere der COMODO-Zertifikate macht sich in den extrem kurzen Ausstellungs- und Supportzeiten, verschiedenen Validierungsvarianten sowie schnellen Handlungsmöglichkeiten bei Problemen deutlich bemerkbar.

Zu guter Letzt sind domainvalidierte Zertifikate nur ein Teil einer gesamten Sicherheitsstrategie. Das Zertifikat sollte nie nach dem Preis, sondern immer nach dem Einsatzzweck ausgewählt werden. Hier gibt es zu den OV, insbesondere aber zu den EV-Zertifikaten einfach keine Alternative.

DV-Zertifikat ist nicht gleich DV Zertifikat

Aufgrund verschiedener Kundenrückfragen wollen wir an dieser Stelle eine klare **Empfehlung** beim Einsatz von domainvalidierten Zertifikaten aussprechen: Das Login SSL Zertifikat von **COMODO** ist nicht nur unser günstigstes Angebot, sondern bietet auch gleich eine doppelte Absicherung: Wer das Zertifikat für domainname.TLD ausstellt, bekommt automatisch die www.domainname.TLD dazu.

CA Whitelist

Zum Schluss noch ein praktischer Tipp:

Es kommt immer wieder zu Verzögerungen bei der Ausstellung der Zertifikate, weil die Bestätigungsemail im SPAM-Filter hängen bleibt.

Setzen Sie einfach die Emailadressen und Domains der CAs auf Ihre Whitelist:

Comodo: noreply_support@comodo.com
Thawte: isp_enrollmentprocess@thawte.com
Rapid SSL: orderprocessing@rapidssl.com
GeoTrust: orderprocessing@geotrust.com

Wir hoffen, Ihnen mit diesem Newsletter ein paar interessante und hilfreiche Informationen zu liefern.

Sprechen Sie uns gerne jederzeit darauf an.

Herzliche Grüße

Ihr



Andreas Janker



Oliver Elste