Wie Sie sich selbst vor Phishing schützen: Empfehlungen von LeaderTelecom

Jeder kann Opfer von Internetbetrug werden. Sei es bei der Nutzung des Onlinebankings, bei Direktzahlungen über das Internet oder beim Online-Shopping mit Kreditkarte – schützen Sie sich mit diesen einfachen Tipps vor Internetbetrug.

Phishing: So fallen Sie nicht darauf herein

Eine Art des Internetbetrugs ist das Phishing. Dabei erspähen Hacker vertrauliche Daten, wie zum Beispiel Nutzernamen und Passwörter, oder Adressen und Kreditkartennummern. Sie gelangen normalerweise an diese Daten, indem Sie gefälschte Internetseiten erstellen, die dem Original sehr ähnlich sehen. Indem die Nutzer dann ihre echten Daten in die gefälschten Seiten eingeben, übermitteln sie den Betrügern unbewusst sämtliche persönlichen Informationen.

Kürzlich berichtete uns ein Nutzer des Bezahldienstes Paypal, wie er Opfer eines solchen Betrugs wurde. Roman wollte eigentlich Geld aus seinen Devisen an sich überweisen, gelangte jedoch auf eine täuschen echte Phishing-Seite im Paypal-Stil. Er verlor dadurch 100.000 Rubel (ca. 1.400 Euro), die ihm von den Betrügern während des Vorgangs gestohlen wurden. Roman erinnerte sich später daran, dass er für die Überweisung auf die Zwei-Faktor-Verifizierung via SMS verzichtet hatte, einen Unterschied zur Original-Website hatte er in dem Moment nicht feststellen können. Grade weil es so schnell geht, sollten Sie Ihre Daten mit allen erdenklichen Mitteln schützen.

Viele Phishing-Seiten sind kaum bis gar nicht von der Original-Website zu unterscheiden. Besonders beim Surfen mit dem Handy wird die Erkennung noch schwieriger. Wie also soll man die Original-Website erkennen, und wissen, dass man ihr vertrauen kann?

Den ersten Unterschied zu einer Phishing-Seite erkennen Sie in der URL, also der Adresse in der Zeile oben im Browser. Es wird dabei von den Hackern versucht, eine ähnliche Adresse zum Original zu finden. Teilweise sind die Websites nur für wenigen Tage aktiv. Statt https://paypal.com/ steht in der Adresszeile zum Beispiel:

·t.paypal.com

·paypal-visa.com

·paypai.co

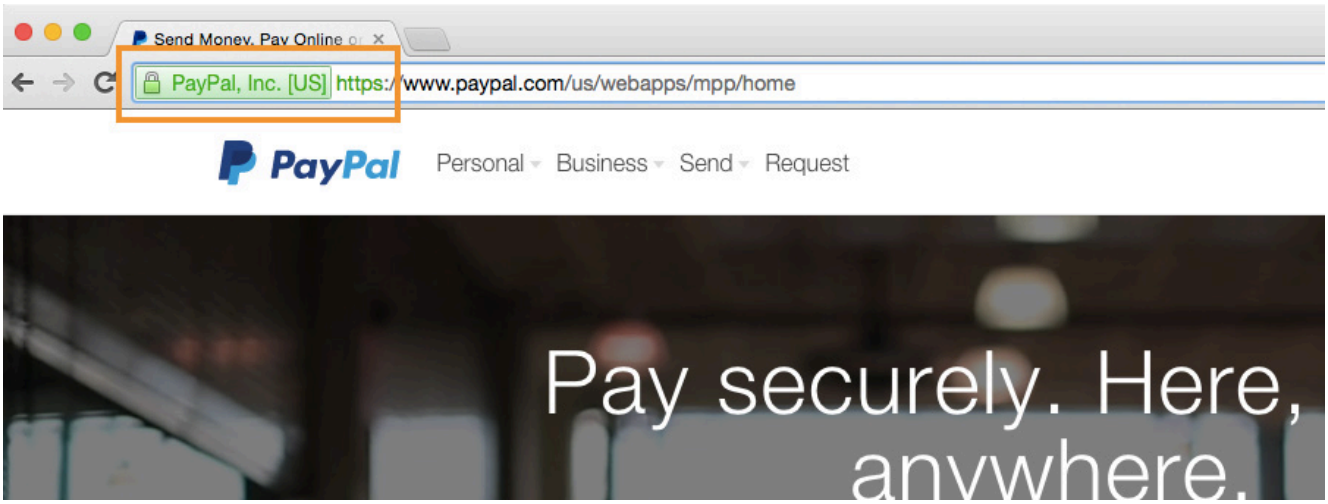
·paypal.hk

·paypl.co

Wie gelangen Internetnutzer auf diese Websites? Vor allem bei der Suche in Suchmaschinen werden die Top-Platzierungen mit Werbemitteln gekauft. Diese bezahlten Links müssen nicht zwingend etwas mit dem eigentlich gesuchten Service zu tun haben, und werden deshalb auch von Hackern genutzt. Weil der Name jedoch ähnlich ist, übersehen einige Nutzer die fehlerhafte URL.

Der zweite Unterschied zu einer Phishing-Seite ist das fehlende SSL-Zertifikat. Heutzutage arbeiten alle Websites, auf denen Sie vertrauliche Daten eingeben können, mit einem HTTPS Protokoll zur sicheren Datenübertragung. Die allermeisten Phishing Websites nutzen hingegen noch das unsichere http-Protokoll. Solchen Seiten können Sie im Hinblick auf eine sichere Datenübertragung grundsätzlich nicht vertrauen.

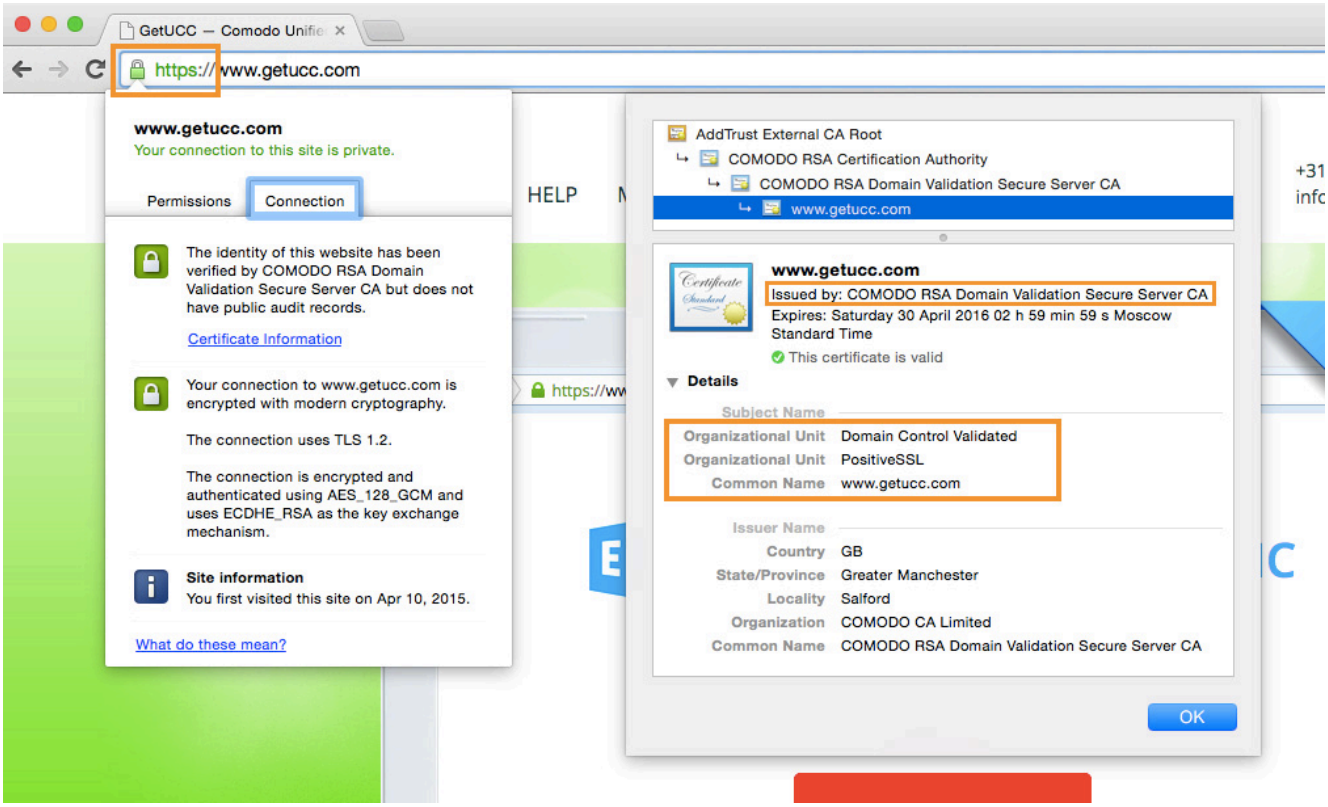
Auf einer sicheren Website sehen Sie ein Schloss-Symbol in der linken Ecke der Adresszeile des Browsers. Wenn Sie auf dieses Symbol klicken, erhalten Sie weitere Details über das Zertifikat.



Leider nutzen zurzeit auch erste Phishing-Seiten eine gesicherte Datenübertragung und das Schloss-Symbol. In diesem Fall gilt es, ein besonderes Augenmerk auf die Art des Zertifikats zu legen: ein DV-Zertifikat schütz zwar die Daten bei der Übertragung, trifft aber keine Aussage über die Echtheit des Unternehmens selbst (z.B. Paypal).

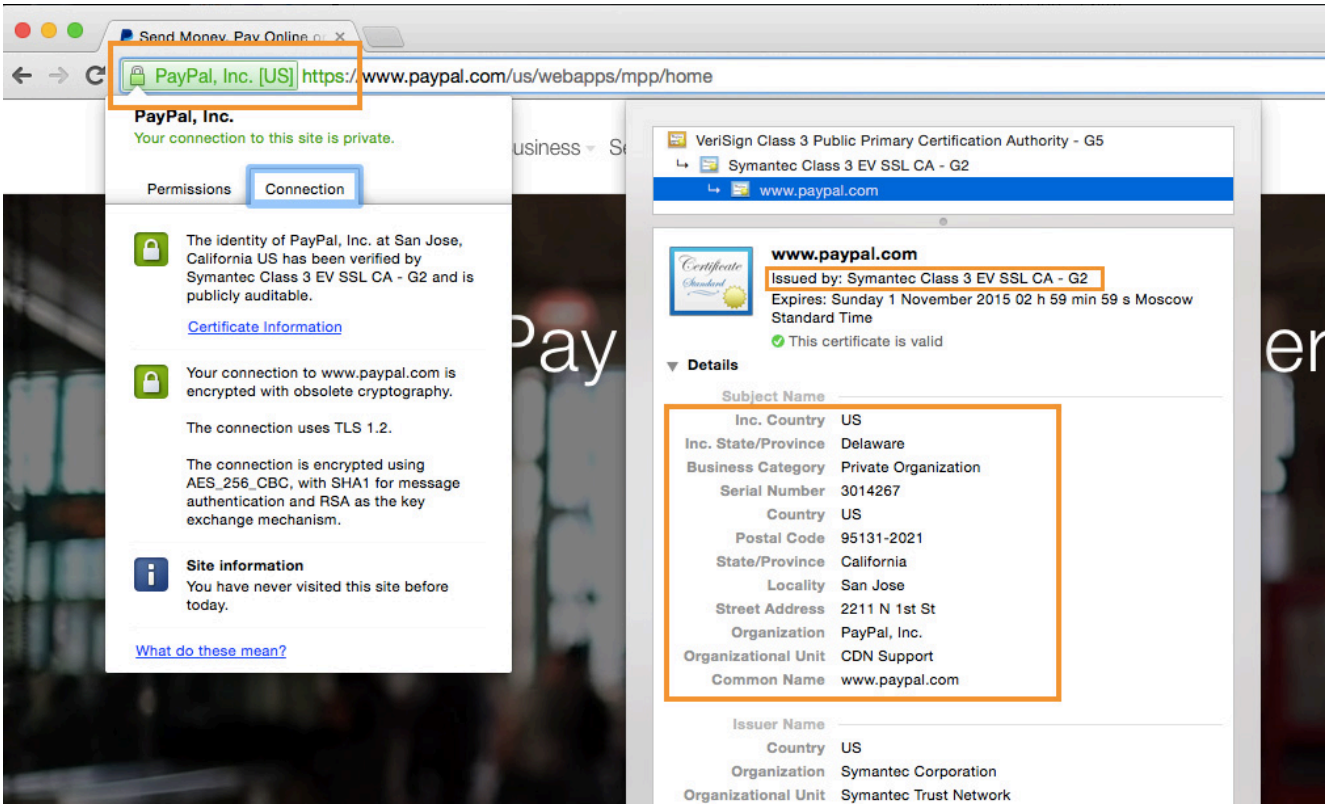
Ein EV-Zertifikat hingegen garantiert nicht nur den sicheren Datenaustausch, es zeigt neben dem Schloss-Symbol auch den Namen des Unternehmens, welches zuvor geprüft wurde. Damit sind EV-Zertifikate die aktuell sichersten und vertrauenswürdigsten Zertifikate.

Zudem färbt das Zertifikat einen Teil der Adresszeile grün und signalisiert damit jedem Nutzer die garantierte Sicherheit dieser Seite.



SSL-Zertifikat: Zum Schutz für Unternehmen

Jedes Unternehmen, welches im Internetdienste anbietet und dabei sensible Nutzerdaten verarbeitet, sollte zum größtmöglichen Schutz der Kunden ein EV SSL-Zertifikat einsetzen.



Durch den Einsatz dieses Zertifikats werden alle Informationen verschlüsselt übertragen, indem sie vor der Übermittlung in eine Buchstaben/Zahlen-Kombination umgewandelt werden. Ein Hacker könnte mit diesem Code nichts anfangen.

Unternehmen mit einem EV-Zertifikat berichten, dass sie ihren Verkauf im Bereich eCommerce zwischen 10-40% steigern konnten – das bestätigen auch unabhängige Analysten. Kaufen Sie Ihr EV-Zertifikat gleich hier.

Was ist SSL?

Was ist SSL?

SSL ist ein Akronym für Secure Sockets Layer. SSL bietet eine sichere Verbindung, mit der Sie private Daten online

übertragen können. Mit SSL gesicherte Websites zeigen ein Vorhängeschloss in der Browser-URL und möglicherweise eine grüne Adressleiste an, wenn sie durch ein EV-SSL-Zertifikat gesichert sind.

Das SSL-Protokoll wird von Millionen von E-Business-Anbietern verwendet, um ihre Kunden zu schützen und sicherzustellen, dass ihre Online-Transaktionen vertraulich bleiben. Um das SSL-Protokoll nutzen zu können, benötigt ein Webserver die Verwendung eines SSL-Zertifikats.

Websites erhalten eine SSL-Verschlüsselung, um alle Bereiche abzudecken, die einen Datenaustausch beinhalten, einschließlich Login-Boxen, Kreditkartenzahlungen oder persönliche Informationen. Alle Webbrowser können mit SSL-gesicherten Websites interagieren, solange das SSL der Websites von einer anerkannten Zertifizierungsstelle wie Comodo stammt.

Warum benötige ich SSL auf meiner Website

Das Internet hat erfolgreich viele neue globale Geschäftsmöglichkeiten für Unternehmen geschaffen, die Online-Handel betreiben. Dieses Wachstum hat jedoch auch Betrüger und Cyberkriminelle angezogen.

Das zunehmende Bewusstsein für Online-Betrüger und Cyberkriminelle bietet E-Commerce-Anbietern die Möglichkeit, die Ängste der Verbraucher zu nutzen, indem sie Vertrauensindikatoren anzeigen. Genau wie in der realen Welt müssen Menschen zuversichtlich sein, bevor sie einen unbekannten Weg einschlagen.

Wie funktioniert SSL?

Wenn ein digitales SSL-Zertifikat auf einer Website installiert ist, sehen Benutzer ein Vorhängeschloss-Symbol im unteren Bereich des Navigators. Wenn ein Extended Validation Certificate auf einer Website installiert ist, sehen Benutzer mit den neuesten Versionen von Firefox, Internet Explorer oder Opera die grüne Adressleiste im URL-Bereich des Navigators.

Benutzern auf Websites mit SSL-Zertifikaten wird während einer E-Commerce-Transaktion auch https:// in der Adressleiste angezeigt.

Wildcard EV-Zertifikate: welche Möglichkeiten gibt es?

Ein EV-Zertifikat ist eine großartige Möglichkeit, Ihre Website vor dem Diebstahl von Benutzerdaten zu schützen. Viele Online-Shops verwenden diese Zertifikate, um das Vertrauen ihrer Kunden in ihre Website noch zu erhöhen. Letztendlich erhalten Sie durch diese Zertifikate für Ihre Website im Browser eine grüne Adresszeile, was Nutzer auf die höchste Sicherheitsstufe beim Browsen hinweist.

Heutzutage wären Website-Betreiber dazu bereit, ein Wildcard EV-Zertifikat zu kaufen, welches eine unbegrenzte Anzahl von Subdomains mit dem grünen Sicherheitssymbol im Browser schützt. Aber solch ein SSL-Zertifikat existiert gar nicht. Hier erfahren Sie die Gründe, und welche Alternativen es gibt.

Warum gibt es keine Wildcard EV-Zertifikate?

EV-Zertifikate bieten die höchste Stufe an Vertrauenswürdigkeit unter allen Arten von SSL-Zertifikaten. Um eine unsachgemäße Anwendung von EV-SSL-Zertifikaten zu vermeiden, verlangt die SSL-Regulierungsbehörde, die für das Aufstellen der Regeln zur Erteilung von SSL-Zertifikaten verantwortlich ist (bekannt als das CA/B Forum), die Überprüfung jedes einzelnen Hosts, der mit einem Zertifikat verbunden ist. Aus diesem Grund ist der Kauf eines Wildcard EV-Zertifikats für unbegrenzte Subdomains nicht möglich. Ein "Wildcard" Zertifikate schützt per Definition eine unbegrenzte Anzahl von Subdomains, die durch ein Sternchen eingebunden sind (z.B. * .domain.com) und nicht explizit aufgelistet werden müssen.

Wenn Sie Ihre Subdomains durch die Anwendung des EV-Zertifikats schützen wollen, können Sie in der Praxis Folgendes tun:

1. Kaufen Sie mehrere separate EV-SSL-Zertifikate.

Diese Möglichkeit ist ideal, wenn Sie nur eine geringe Anzahl von Subdomains haben, die Sie schützen wollen. In diesem Fall können Sie für jede Subdomain ein einzelnes EV-Zertifikat ausstellen. Der Nachteil dieser Option ist, dass Sie wahrscheinlich (abhängig davon, wo Sie den Auftrag erteilen) die notwendigen Daten für jedes einzelne Zertifikat separat eingeben müssen. Das ist für den Nutzer etwas unpraktisch. Solche EV-Zertifikate können SIe auf der LeaderTelecom Website bestellen.

2. Kaufen Sie ein EV Multi-Domain Zertifikat.

Diese Option ist günstiger, weil das Multi-Domain-Zertifikat eine ausreichend große Anzahl von Domains (einschließlich Subdomains) abdeckt. Der Kauf dieses Zertifikats ist sehr

rentabel, wenn Sie viele Domains / Subdomains haben, die Sie damit schützen wollen. Je mehr Domainnamen Sie hinzufügen, umso effizienter wird das Multi-Domain-Zertifikat im Vergleich zum Standard EV-Zertifikat. Außerdem braucht der Nutzer nur einen Antrag für ein Zertifikat stellen, in dem alle Domainnamen enthalten sind. Damit kann er viel Zeit sparen.

Zusätzliche Domainnamen können dem Zertifikat hinzugefügt werden, auch nachdem es bereits ausgestellt wurde. Das ist dann besonders günstig, wenn einer Ihrer Domainnamen noch nicht bekannt ist. Auch das EV-Multi-Domain-Zertifikat können Sie auf der LeaderTelecom Website bestellen.

Ein weiterer Vorteil des Multi-Domain-Zertifikats gegenüber separaten EV-Zertifikaten ist die einfache Verwaltung. Es ist viel einfacher, ein einzelnes Multi-Domain-Zertifikat zu verwalten als mehrere einzelne Zertifikate. Außerdem können Sie durch Multi-Domain-Zertifikate Geld sparen (mehr Websites, mehr Ersparnis). Aus diesen Gründen kaufen bereits immer mehr Betreiber mehrerer Websites ein Multi-Domain-EV-Zertifikat. Ein solches EV-Multi-Domain-Zertifikat können Sie jederzeit auf der LeaderTelecom Website mit einem guten Rabatt kaufen.

Unterschied zwischen DV- und OV-Zertifikaten

Wir wissen bereits, dass man SSL-Zertifikate in drei Typen unterteilt: DV, OV und EV. In diesem Artikel erklären wir die ersten beiden Zertifikate, DV und OV. Erfahren Sie im Folgenden mehr über ihre Unterschiede und Einsatzmöglichkeiten, und wann Sie welches Zertifikat benötigen.

Bei einem DV-Zertifikat steht die Abkürzung für Domain Validation, das bedeutet eine Validierung/Überprüfung der Domain. Dies ist das grundlegende Level für ein SSL-Zertifikat. Eine Zertifizierungsstelle (Certification Authority (CA)) bestätigt damit, dass Sie der Inhaber einer bestimmten Domain sind, und damit die Informationen des WHOIS-Eintrags. Dieses Zertifikat erlaubt selbstverständlich wie gewünscht eine sichere Datenverschlüsselung auf Ihrer Website, aber es verifiziert Sie nicht als Besitzer eines rechtmäßigen Unternehmens. Trotzdem ist dies ein absolut zulässiges Zertifikat und eine sehr schnelle Lösung für den effektiven Schutz einer Website per HTTPS. Dank des weit bekannten Schloss-Symbols neben der Adressleiste im Browser werden Kunden Ihrer Website im höheren Maße als vorher vertrauen.

Beispiel für ein DV-Zertifikat:

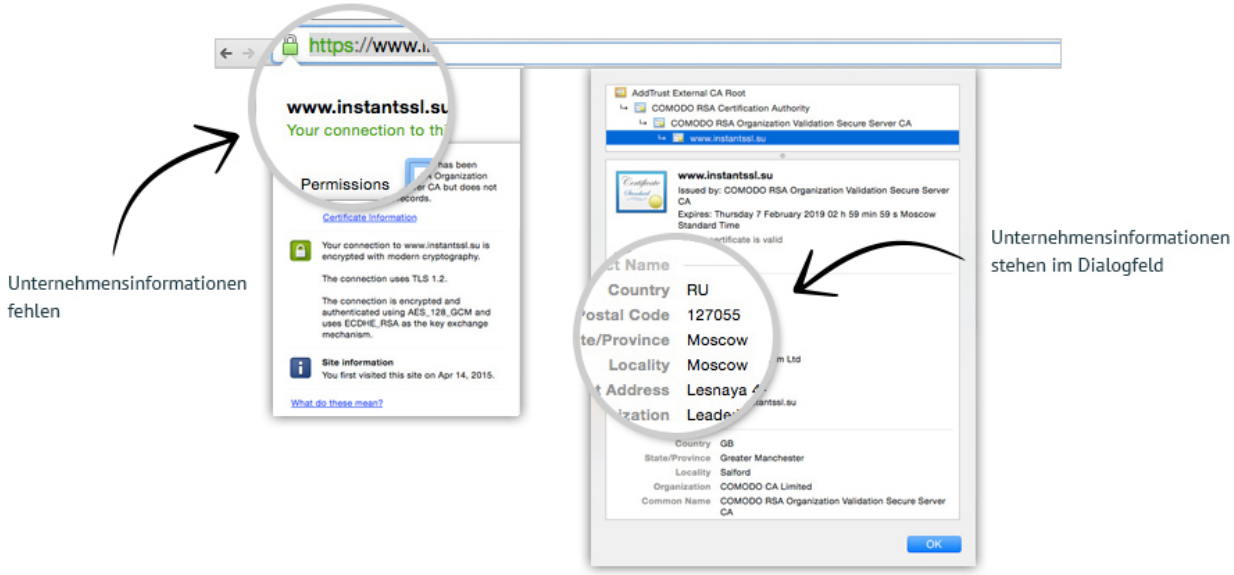
Ein DV-Zertifikat bietet sich überall da an, wo Sicherheit eine wichtige, aber keine übergeordnete Rolle spielt. Denn auch Internetbetrügern und Hackern ist es leider möglich, DV-Zertifikate für Ihre gefälschten Phishing-Seiten zu verwenden. Hier werden arglose Nutzer mittels des vermeintlich sicheren Schloss-Symbols dazu verleitet, ihre persönlichen Daten anzugeben, welche dann in die Hände der Kriminellen fallen. Nur weil die Datenübertragung verschlüsselt wird heißt das nämlich nicht, dass die Daten auch beim richtigen Empfänger ankommen. Internetnutzer müssen deshalb auch sichergehen können, dass die aufgerufene Website auch zu einem rechtmäßigem Unternehmen gehört, bevor sie einen Kauf abschließen oder private Daten angeben.

Aus diesem Grund empfehlen wir für Websites mit höchsten Sicherheitsansprüchen ein OV-Zertifikat.

Ein OV-Zertifikat als Abkürzung für Organisation Validation, also mit einer Überprüfung des Unternehmens, benötigen vor allem Firmen und Organisationen, bei denen Kunden sensible

Daten (Kreditkartennummern, Kontaktdaten, etc.) angeben müssen. Sie eignen sich damit insbesondere für eCommerce-Seiten und jede Art von Onlineverkauf. Ein OV-Zertifikat beglaubigt die Echtheit des Inhabers einer Website und benötigt dafür rechtmäßige Unternehmensinformationen von einer Firma. Der Validierungsprozess für solche Zertifikate dauert deshalb etwas länger und ist umfangreicher. Die Zertifizierungsstelle bescheinigt nicht nur, dass Ihnen die entsprechende Domain gehört, sondern auch, dass Sie der rechtmäßige Besitzer des Unternehmens sind. Dafür muss die Firma in einem Unternehmensregister und einem Onlineverzeichnis gelistet sein, zum Beispiel dnd.com. Kriminelle können kein solches OV-Zertifikat bekommen, weil sie ihre „Firma“ nicht rechtmäßig überprüfen lassen können. Der Hauptvorteil eines OV-Zertifikats liegt darin, dass Ihr Unternehmen auf dem Zertifikat namentlich genannt wird.

Beispiel für ein OV-Zertifikat:



Erwägen Sie den Wechsel von einem DV-Zertifikat auf ein OV-Zertifikat, wenn:

- Sie sensible Nutzerdaten schützen müssen
- der Name Ihres Unternehmens auf dem Zertifikat stehen soll (für ein höheres Vertrauen der Nutzer)

- Sie Ihre Geschäftstätigkeiten ausweiten und auf ein neues Level heben möchten
- Nutzer Ihre Website als rechtmäßiges Unternehmen und keinesfalls als Phishing-Seite wahrnehmen sollen

Wenn Sie noch Fragen zu einem Zertifikatswechsel haben, oder überlegen von einem DV- auf ein OV-Zertifikat umzusteigen, fragen Sie unsere Experten von LeaderTelecom. Mit unserer jahrelangen Erfahrung und schlanken Prozessen bei der Kommunikation mit den Zertifizierungsstellen stellen wir Ihnen jede Art von Zertifikat komfortabel und schnell aus.

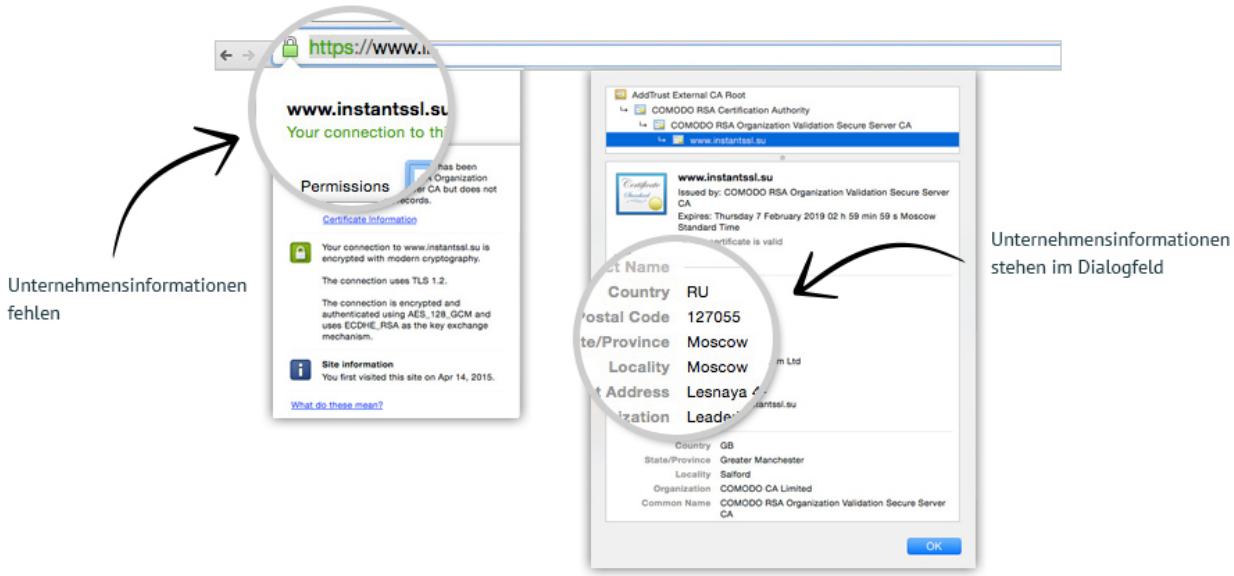
Unterschied zwischen OV- und EV-Zertifikaten

SSL-Zertifikate sind heutzutage eine wesentliche Voraussetzung für eCommerce-Seiten. Schwer vorstellbar, dass eine glaubwürdige Unternehmensseite nicht sicher sein könnte. Jeder Zweifel würde einen Kunden davon abhalten, auf einer solchen Seite einen Onlinekauf zu tätigen. Aus diesem Grund sollten Sie als Inhaber eines rechtmäßigen Unternehmens mit einem Online-Shop auf jeden Fall über den Einsatz eines SSL-Zertifikats nachdenken. Dabei stellt sich vielen Domain-Inhabern die Frage: Welcher Zertifikatstyp ist der richtige, OV oder EV? Und wo liegt der Unterschiede zwischen diesen beiden SSL-Zertifikaten?

Ein OV-Zertifikat mit der Abkürzung OV für Organisation Validation, was sich mit Unternehmensüberprüfung übersetzen lässt, verifiziert die Echtheit einer Organisation oder einer Firma. Für das Ausstellen eines OV-Zertifikats muss ein Unternehmen zunächst den Validierungsprozess abschließen.

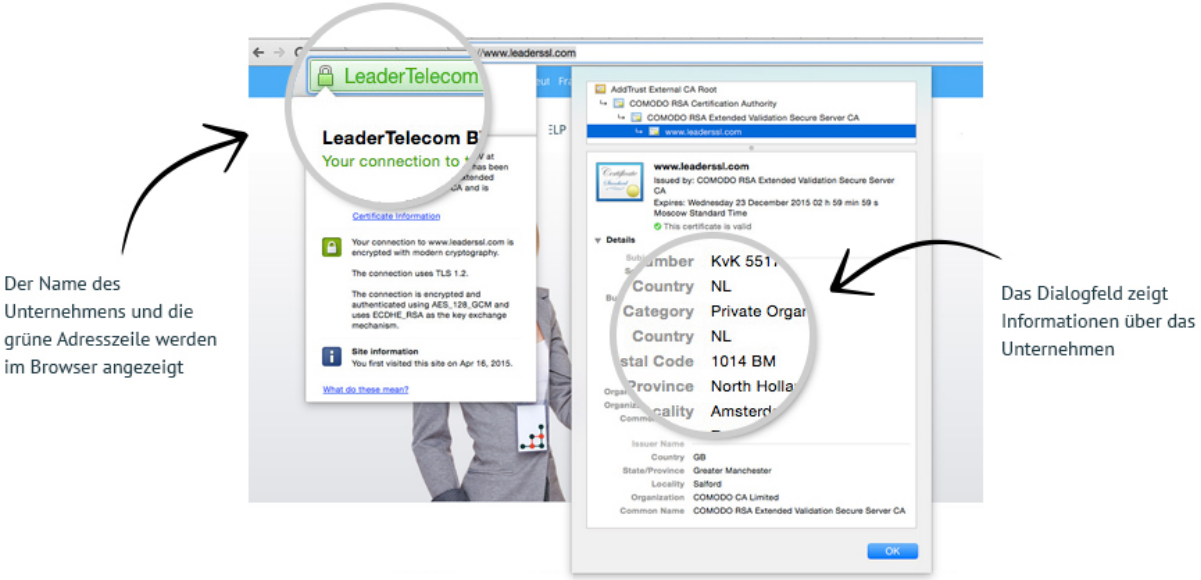
Darin bestätigt die Zertifizierungsstelle die Existenz des Unternehmens mittels eines Abgleichs mit einem staatlicher Unternehmensregister und einem Onlineverzeichnis. Sobald die gewünschte Website per OV-Zertifikat gesichert ist, sehen die Internetnutzer das bekannte Schloss-Symbol neben der Adressleiste im Browsers und wissen damit um den Schutz der Seite vor Hackern.

Beispiel für ein OV-Zertifikat:



EV-Zertifikate, welche für Extended Validation, also eine erweiterte Überprüfung stehen, gelten derzeit als sicherste und vertrauenswürdigste Lösung für die weltweit führenden Online-Unternehmen. Das Zertifikat beinhaltet das Anzeigen einer grünen Browser-Adresszeile als Zeichen für Sicherheit und Zuverlässigkeit. Außerdem wird auch der Name des Unternehmens bei einem EV-Zertifikat direkt im Browserfenster mit angezeigt, wie Sie auf dem Screenshot unten sehen können. Damit erfassen Internetnutzer schnell, dass diese Website von einer rechtmäßigen Firma und nicht von Hackern betrieben wird. Das Ausstellen eines EV-Zertifikats ist nicht viel aufwendiger, als das Vorgehen bei einem OV-Zertifikat – trotzdem bietet es eine höhere Stufe an Sicherheit und Vertrauen. Dank des Zertifikats fühlen sich Internetnutzer beim Surfen aus Ihrer Website sicherer, und das gesteigerte Vertrauen wird Ihre Verkaufszahlen ankurbeln.

Beispiel für ein EV-Zertifikat:



- EV-Zertifikate beinhalten ein grafisches Symbol (die grüne Adresszeile im Browser), als bewährtes Zeichen für Glaubwürdigkeit selbst für unerfahrene Internetnutzer
- EV-Zertifikate zeigen den Namen des Unternehmens (direkt in der Adresszeile des Browsers) und weiterführende Informationen darüber an
- EV-Zertifikate sind nicht viel teurer als OV-Zertifikate, haben aber mehr Vorteile
- EV-Zertifikate werden von weltweit tätigen Unternehmen bevorzugt

Falls Sie den Wechsel zu einem EV-Zertifikat in Betracht ziehen, sich aber noch vor dem Validierungsprozess scheuen, sprechen Sie uns gerne an! Gerne übernehmen unsere Experten von LeaderTelecom diese Aufgabe für Sie. Mit unserer jahrelangen Erfahrung und vielfach bewährten Prozessen helfen wir Ihnen in kürzester Zeit zu einem eigenen EV-Zertifiakt.