



STRATEGIEPAPIER

DER AKTUELLE STAND VON SSL-LÖSUNGEN FÜR DIE ONLINE-SICHERHEIT

INHALT

- 1 EINLEITUNG
- 1 ÜBERBLICK
- 2 EXTENDED VALIDATION (EV) SSL: GOLDSTANDARD DER AUTHENTIFIZIERUNG
- 3 VERTRAUENSMARKEN SCHAFFEN KUNDENVERTRAUEN
- 3 BEKANNTE VERTRAUENSMARKEN GARANTIEREN VERTRAUENSWÜRDIGKEIT
- 3 VERTRAUENSMARKEN KÖNNEN NOCH MEHR: VERISIGN® SEAL-IN-SEARCH™
- 4 SERVER GATED CRYPTOGRAPHY (SGC) - DAMIT ALLE BESUCHER VON EINER STARKEN VERSCHLÜSSELUNG PROFITIEREN
- 4 SCHLUSSFOLGERUNG
- 4 VERISIGN



DER AKTUELLE STAND VON SSL LÖSUNGEN FÜR DIE ONLINE- SICHERHEIT

EINLEITUNG

„Secure Sockets Layer“, besser bekannt unter der Abkürzung SSL, ist de facto der Standard für Sicherheit im Online-Handel. SSL unterbindet Gefahren wie Ausspähen und Missbrauch vertraulicher Daten, Datenmanipulation, Phishing und andere Formen von Online-Kriminalität mit Hilfe der Verschlüsselung – so sind die Daten nur für den vorgesehenen Empfänger lesbar. Da SSL-Zertifikate nur nach einer Überprüfung des Antragstellers ausgestellt werden, profitieren die Besucher Ihrer Website davon überdies auch, weil sie sicher sein können, dass die Website vertrauenswürdig ist. Alle gängigen Betriebssysteme, Webanwendungen, Browser und Server unterstützen SSL, das mit seiner leistungsstarken Verschlüsselung und der Authentifizierung einen systemweiten Schutz bietet. Ihr Unternehmen kann damit das Vertrauen seiner Kunden erlangen und bewahren, den Anteil tatsächlich abgeschlossener Geschäftstransaktionen steigern und unter dem Strich das Geschäftsergebnis verbessern.

SSL und dazugehörige Technologien wurden in letzter Zeit weiter verbessert und so decken die verschiedenen derzeit erhältlichen SSL-Produkte eine große Bandbreite an Funktionen ab. Dieses Strategiepapier erläutert einige dieser Weiterentwicklungen, damit Sie fundiert entscheiden können, welche Lösung für Ihr Unternehmen am besten geeignet ist.

ÜBERBLICK

SSL wurde Mitte der 1990er Jahre von VeriSign mit dem Ziel auf den Markt gebracht, den abhörgeschützten Austausch von Daten über das Internet zu ermöglichen. Ein SSL-Zertifikat ist eine Datei, die individuell für ein Unternehmen zum Einsatz auf einer bestimmten Domain auf einem bestimmten Server generiert wird. SSL-Zertifikate werden – ähnlich wie Personalausweise oder Führerscheine – von vertrauenswürdigen Genehmigungsinstanzen ausgegeben, den Zertifizierungsstellen (CA). Ein Unternehmen erhält ein SSL-Zertifikat nur, wenn es eine Überprüfung durch die CA bestanden hat, bei der unter anderem Identität und

Legitimität des Antragstellers überprüft werden. Angesichts der enormen Zunahme von Phishing-Versuchen und anderen Formen von Betrug, deren Ziel es ist, vertrauliche Daten auszuspähen, ist die Authentifizierung der Identität wichtiger als je zuvor.

SSL verwendet ein System mit privatem und öffentlichem Schlüssel zur Verschlüsselung des Datenaustauschs zwischen zwei Stellen, beispielsweise einem Kunden und einer Website mit SSL-Zertifikat. Wenn der Kunde die mit SSL gesicherte Website in seinem Browser aufruft, führen die beiden Systeme zur gegenseitigen Authentifizierung einen sogenannten „Handshake“ durch. In jeder Sitzung wird ein eigener Schlüssel verwendet, und je länger die Bit-Länge dieses Schlüssels ist, desto stärker ist die Verschlüsselung. Sobald die Verbindung hergestellt wurde, ist gewährleistet, dass die zwischen beiden Seiten ausgetauschten Daten sicher sind und nicht manipuliert werden können. Dies ist besonders dann wichtig, wenn sensible und vertrauliche Daten über das Internet, ein Extranet oder ein Intranet ausgetauscht werden. Für den Online-Handel ist eine sichere SSL-Verbindung eine Grundvoraussetzung, denn ein Großteil der Internetbenutzer ist nicht bereit, solche Daten auf Websites anzugeben, die nicht durch SSL geschützt sind.

Kunden kaufen im Internet oft nur Kleinigkeiten von unterschiedlichen Anbietern und tun sich allgemein schwer damit, eingefahrene Kaufgewohnheiten zu ändern oder vertrauliche Angaben zu machen – all dies sind Verhaltensweisen, die das Erfolgspotenzial im Online-Handel einschränken. Um diesen Hemmnissen entgegenzuwirken, müssen Online-Anbieter das Vertrauen ihrer Kunden und Interessenten gewinnen. Auf den folgenden Seiten lernen Sie einige Funktionen kennen, die Sie bei der Wahl einer SSL-Lösung für Ihr Unternehmen berücksichtigen sollten.



EXTENDED VALIDATION (EV) SSL: GOLDSTANDARD DER AUTHENTIFIZIERUNG

Zwar sind immer mehr Menschen gerne online, aber zwischen der Anzahl der „Surfer“ und der Anzahl derjenigen, die bereit sind, online Transaktionen durchzuführen, klafft eine große Lücke. Der Grund hierfür liegt in der Angst vor der Kompromittierung vertraulicher Daten. In einer Umfrage, die TNS im März 2010 im Auftrag von VeriSign durchgeführt hat, gaben vierzig Prozent der Befragten an, sie würden aufgrund von Sicherheitsbedenken niemals Rechnungen online bezahlen oder Online-Banking nutzen, und rund ein Drittel lehnte es aus denselben Gründen ab, online einzukaufen oder Geldanlagen zu verwalten.

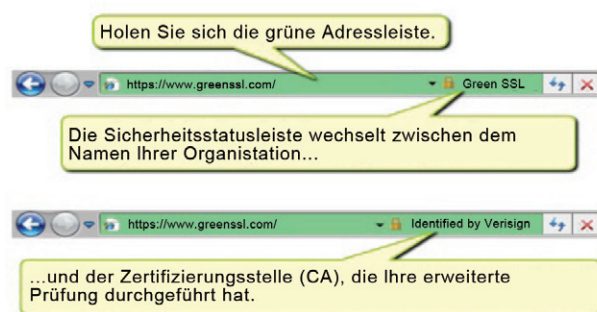
Keine Frage, die Anzahl der potenziellen E-Commerce-Kunden, die davor zurückschrecken, vertrauliche persönliche oder finanzielle Daten einem abstrakten und gesichtslosen Gegenüber offenzulegen, ist zu hoch. Diese Menschen brauchen die Gewissheit, dass ihre vertraulichen Daten auch vertraulich bleiben, und verlangen immer häufiger Belege für ausreichende Sicherheitsmaßnahmen, bevor sie solche Daten eingeben oder online Transaktionen durchführen.

Diese Situation gab den Anlass für eine Reihe von CAs, Browseranbietern und WebTrust-Prüfern, das CA/Browser-Forum ins Leben zu rufen, um einen neuen SSL-Standard zu schaffen – einen, der Online-Kunden sofort überzeugt und den sie gerne annehmen. Dieses Konsortium, dem unter anderem Vertreter von Microsoft und VeriSign angehören, hat die Authentifizierung mit Extended Validation (EV) entwickelt. Dieser neue Branchenstandard soll die Zunahme von Internetbedrohungen wie Phishing-Angriffen bekämpfen.

Um ein SSL-Zertifikat mit EV zu erhalten, müssen die Antragsteller ihr Unternehmen und ihre Website von der CA nach wesentlich strengeren Kriterien überprüfen lassen. Aus diesem Grund gilt EV SSL in der E-Commerce-Branche als „Goldstandard“ zur Bestätigung der Legitimität und Identität einer Website. Bevor eine CA SSL-Zertifikate mit EV ausstellen darf, muss sie selbst eine eingehende Überprüfung durch WebTrust bestehen. VeriSign wirkt weiterhin federführend bei der Entwicklung und Implementierung von EV SSL mit.

Ein SSL-Zertifikat mit EV bietet Unternehmen und Kunden einen anerkannten und angesehenen Schutz vor immer ausgefeilteren Betrugsmethoden. Bestandteil von EV SSL sind bestimmte optische Merkmale, anhand derer Kunden

eine Website mit EV SSL bereits auf den ersten Blick als solche erkennen können. Browser mit entsprechenden Sicherheitsmerkmalen zeigen die Zertifizierung mit SSL EV anders an als die mit herkömmlichem SSL. Auf einer Website, für die ein SSL-Zertifikat mit EV vorliegt, färbt sich die Adressleiste in diesen Browsern grün und in einem eigenen Feld werden der Name des Website-Eigentümers sowie der Name der Genehmigungsinstanz, also der CA, die das SSL-Zertifikat mit EV ausgestellt hat, angezeigt.



Die Richtlinien für die Ausgabe von SSL-Zertifikaten mit EV bieten Kunden und Website-Betreibern zusätzlichen Schutz, denn sie verpflichten die CA zu einer vom CA/Browser-Forum klar definierten Vorgehensweise. Diese festgeschriebene und gleichbleibende Vorgehensweise minimiert die Möglichkeit der Ausstellung von Zertifikaten an Empfänger, die den Vorgaben nicht genügen, wodurch das Maß an Sicherheit wieder sinken würde.

Im April 2010 haben Unternehmen in aller Welt in über 30 Tests gezeigt, dass mit dem Einsatz von VeriSign® EV SSL-Zertifikaten die Anzahl der Transaktionen um durchschnittlich 17,8 Prozent steigt.² Um nur einige Beispiele der von unseren Kunden mit VeriSign EV SSL erzielten Erfolge herauszugreifen:

Messbare Ergebnisse mit VeriSign EV SSL-Zertifikaten

Papercheck.com: 87 % mehr Online-Registrierungen

CRSHotels.com: 30 % höhere Abschlussrate

CarlInsurance.com: 18 % mehr Online-Abschlüsse

Flagstarbank.com: 10 % mehr Neukunden

CreditKarma.com: 26 % höhere Abschlussrate

Die genauen Ergebnisse finden Sie unter <http://www.verisign.de/ssl/ssl-information-center/ssl-case-studies/index.html>.



Ebenso wie herkömmliche SSL-Zertifikate ermöglichen auch SSL-Zertifikate mit EV die sichere, verschlüsselte Kommunikation zwischen Website und Browser. Bestätigt wird außerdem die Echtheit der Website, so dass die Besucher wissen, dass sie sich tatsächlich auf der gewünschten Website befinden und nicht etwa auf einer gefälschten.

VeriSign ist der weltweit führende Anbieter von SSL-Zertifikaten. Heute sind Extended Validation SSL-Zertifikate bei über 24.000 Websites im Einsatz, und mehr als 17.000 dieser Zertifikate stammen von VeriSign.³

VERTRAUENSMARKEN SCHAFFEN KUNDENVERTRAUEN

Praktisch alle Kunden machen sich Sorgen wegen Identitätsdiebstahl, Kreditkartenbetrug und anderen Bedrohungen im Internet – und das mit gutem Grund. Die Bedrohung durch Phishing bleibt akut und nimmt weiterhin zu. Im Oktober 2009 erreichte die Anzahl gekapertter Marken die Rekordzahl von 356, ein Anstieg um fast 4,4 Prozent gegenüber der bisherigen Höchstmarke von 341 im August 2009.⁴

Es ist davon auszugehen, dass das Wissen über Sicherheitslösungen bei Kunden zunehmen wird, denn sowohl Unternehmen aus der Internetsicherheitsbranche als auch Behörden bemühen sich, ein Bewusstsein für Notwendigkeit von Sicherheitsmaßnahmen zu schaffen. Es lässt sich schon jetzt feststellen, dass Online-Kunden immer besser über Sicherheitsfragen Bescheid wissen. Vielfach wird bereits erwartet, dass Online-Shops durch bekannte Vertrauensmarken als sichere Wahl für den sorgenfreien Einkauf gekennzeichnet sind. Die Anzeige einer bekannten Vertrauensmarke auf der Website ist daher zu einer unverzichtbaren Voraussetzung geworden, damit aus dem Online-„Schaufensterbummel“ ein abgeschlossener Kauf wird.

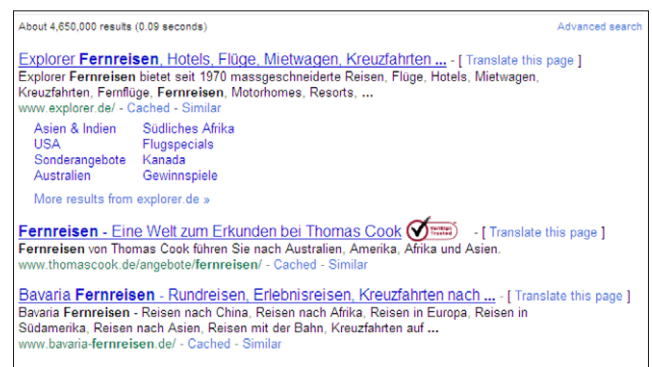
BEKANNTE VERTRAUENSMARKEN GARANTIEREN VERTRAUENSWÜRDIGKEIT

Untersuchungen zeigen nicht nur, dass die meisten Online-Kunden das VeriSign-Siegel kennen, sondern auch, dass dieses Siegel den Grund für die Kaufentscheidung liefern

kann. Das VeriSign-Siegel wird Tag für Tag über 250 Millionen Mal gesehen und ist 68 Prozent der Online-Kunden der Online-Kunden in Europa kennen das VeriSign Secured Seal besser als jedes andere Vertrauenszeichen.⁵ Beim Kauf eines VeriSign SSL-Zertifikats erwerben Sie auch die Berechtigung, mit dem VeriSign Trust™ Siegel an auffälliger Stelle auf Ihrer Website und in Suchergebnissen zu werben. Damit erhöhen Sie das Vertrauen der Kunden in Ihre Website und möglicherweise ebenfalls die Anzahl der abgeschlossenen Transaktionen.

VERTRAUENSMARKEN KÖNNEN NOCH MEHR: VERISIGN® SEAL-IN-SEARCH™

Es wird immer wichtiger, Kunden so früh wie möglich in ihrem Entscheidungsprozess zu erreichen und sie auf die Vertrauenswürdigkeit einer Website aufmerksam zu machen. Wenn in den Suchergebnissen neben Ihrem Link eine Vertrauensmarke angezeigt wird, ist das sofort eine Auszeichnung. Diese Funktion nennt sich VeriSign® Seal-in-Search™. Damit können Unternehmen Interessenten bereits Vertrauenswürdigkeit signalisieren, wenn diese noch gar nicht auf ihrer Website sind. Beim Suchen und Vergleichen von Angeboten klicken Interessenten häufig auf Links mit einer Vertrauensmarke. Indem Sie auf diese Weise potenziellen Kunden Ihre Vertrauenswürdigkeit signalisieren, verbessern Sie die Ausgangsposition Ihrer Website und damit auch Besucherzahlen und Umsatz.



Durch die Anzeige von Vertrauensmarken können Unternehmen schon in den Suchergebnissen auf ihre Vertrauenswürdigkeit hinweisen und die Zahl der Besucher Ihrer Website steigern.

3. Netcraft Survey, May 2010

4. [www.antiphishing.org](#)

5. "VeriSign 2009 Brand Research", Synovate/GMI, May 2009 (Auf English



SERVER GATED CRYPTOGRAPHY (SGC) – DAMIT ALLE BESUCHER VON EINER STARKEN VERSCHLÜSSELUNG PROFITIEREN

SGC (Server Gated Cryptography) gibt es schon länger als SSL-Erweiterung. Dieses Verfahren sorgt dafür, dass die empfohlene Verschlüsselungsstärke von mindestens 128 Bit verwendet werden kann, unabhängig von der Verschlüsselungsstärke, die der Browser des Kunden von Haus aus mitbringt, denn mit SGC wird die Verschlüsselungsstärke ausschließlich vom Server vorgegeben, nicht vom Browser. Ohne SGC wird automatisch die niedrigste von Server und Browser unterstützte Verschlüsselungsstärke verwendet. Da Experten für alle sicheren Online-Verbindungen generell eine Verschlüsselungsstärke von mindestens 128 Bit empfehlen, kommt SGC besonders dann zum Tragen, wenn Kunden alte Browserversionen verwenden, die die Verschlüsselung mit 128 Bit noch nicht unterstützen.

Vom Marktführer VeriSign erhalten Sie SSL-Zertifikate mit SGC und können so dafür sorgen, dass praktisch alle Besucher Ihrer Website die empfohlene Mindestverschlüsselungsstärke von 128 Bit nutzen können.

SCHLUSSFOLGERUNG

Vertrauenswürdigkeit ist ein wichtiger Baustein der Sicherheit im Internet. VeriSign ist derzeit die weltweit anerkannteste Marke für Internetsicherheit. Dieses Ansehen bei Privat- und Firmenkunden hat sich VeriSign über viele Jahre durch seine innovativen Spitzenleistungen und die Einbindung modernster Verfahren in seine hochwertigen SSL-Lösungen erarbeitet. EV SSL und Seal-in-Search sind nur zwei Beispiele aus jüngerer Zeit, die das Engagement belegen, mit dem VeriSign den Schutz vor den immer wieder neuen Angriffsversuchen aus dem Internet kontinuierlich weiterentwickelt. Wenn Sie möchten, dass Ihre Kunden zum Online-Einkauf voller Vertrauen zu Ihnen kommen, entscheiden Sie sich für SSL-Zertifikate von VeriSign.

VERISIGN

VeriSign ist führender Anbieter von Internetinfrastrukturdiensten für die digitale Welt. Milliardenfach pro Tag verlassen sich Unternehmen und Kunden bei vertrauensvoller Kommunikation und sicherem Handel auf unsere Internetinfrastruktur.

Weitere Informationen erhalten Sie unter www.Verisign.de.

