VeriSign®

STRATEGIEPAPIER

Die allerneuesten Entwicklungen in der SSL-Technologie

INHALT

Die allerneuesten Entwicklungen in der SSL-Technologie

+ Einleitung

Secure Sockets Layer (SSL) ist der weltweite Standard für Web-Sicherheit. Um unbefugten Zugriff auf vertrauliche Informationen, Datenmanipulation, Datenraub, *Phishing* und andere Formen des Online-Betrugs zu verhindern, werden vertrauliche Daten mit Hilfe der SSL-Technologie so verschlüsselt, dass nur autorisierte Empfänger sie lesen können. Neben dem Schutz vertraulicher Daten bietet SSL den Benutzern Ihrer Website zudem die Sicherheit, auf eine gültige Website zuzugreifen. SSL-Unterstützung ist in alle wichtigen Betriebssysteme, Web-Anwendungen sowie die Server-Hardware integriert, sodass die leistungsstarke SSL-Verschlüsselungstechnologie für einen systemweiten Schutz Ihres Unternehmens sorgt und damit zur Stärkung des Vertrauens Ihrer Kunden, mehr abgeschlossenen Transaktionen und letztendlich zur Umsatzsteigerung beiträgt. Dank der neuesten Entwicklungen in der SSL-Technologie stehen Ihnen verschiedene SSL-Typen zur Verfügung. In diesem Strategiepapier werden wir einige dieser Entwicklungen erläutern, damit Sie entscheiden können, welcher SSL-Typ sich am besten für Ihr Unternehmen eignet.

+ Übersicht über SSL

SSL ist seit mehr als 10 Jahren der Verschlüsselungsstandard für den Schutz von Online-Kommunikation. Eine spezifische Datendatei, das SSL-Zertifikat, wird dabei für einen bestimmten Server in einer bestimmten Domäne für ein bestimmtes Unternehmen erstellt. Wie ein Ausweis oder ein Führerschein wird auch ein SSL-Zertifikat von einer vertrauenswürdigen Stelle, z. B. VeriSign, ausgestellt. Jede Dateneinheit wird authentifiziert, d. h. es wird überprüft, ob es sich auch wirklich um die angegebene Dateneinheit handelt, bevor sie ein SSL-Zertifikat erhält. Da Phishing und andere Formen des Online-Betrugs, bei denen persönliche Daten ausspioniert werden, explosionsartig zugenommen haben, ist die Authentifizierung der Identität heutzutage wichtiger als je zuvor. Das Niveau der Identitätsauthentifizierung ist jedoch von SSL-Zertifikat zu SSL-Zertifikat und von Zertifizierungsstelle (CA) zu Zertifizierungsstelle verschieden.

Bei SSL wird die Verbindung zwischen zwei Parteien, z. B. zwischen einem Kunden und einer Website mit SSL-Zertifikat, von einem privaten und einem öffentlichen Verschlüsselungssystem verschlüsselt. Wenn im Browser eines Kunden eine SSL-gesicherte Website aufgerufen wird, werden beide Parteien durch einen sogenannten „Handshake“ authentifiziert. Für jede Sitzung wird ein eindeutiger Sitzungsschlüssel verwendet (je länger der Schlüsselcode, desto sicherer die Verschlüsselung). Sobald diese Verbindung hergestellt wurde, können beide Parteien an einer sicheren Sitzung teilnehmen, bei der Datenschutz und Integrität der Kommunikation gewährleistet sind. Diese Sicherheitsstufe ist besonders wichtig, wenn vertrauliche Informationen über das Internet, ein Extranet oder selbst innerhalb eines Intranets ausgetauscht werden. Bei E-Commerce ist eine sichere SSL-Verbindung unternehmenswichtig, da die meisten Internetbenutzer ihre Daten nicht einer Website anvertrauen möchten, die keinen SSL-Schutz bietet.

Eine kleine Anschaffung hier, eine kleine Anschaffung dort – die große Masse der Online-Kunden ändert ihre Einkaufsgewohnheiten nur widerwillig und gibt ebenso ungern persönliche Informationen preis. Da stellt sich die Frage: Werden sich potenzielle Kunden bei Online-Geschäften mit Ihrer Website sicher genug fühlen, um den Sprung in die Welt der Online-Transaktionen zu wagen?

+ Server Gated Cryptography (SGC): Hocheffektive Verschlüsselung für die meisten Websitebesucher

Wenn Ihr Ruf in der Online-Gemeinde davon abhängt, wie sicher die Verarbeitung von Informationen über Ihre Website ist, sollte Ihre Internetsicherheitslösung für jeden Besucher der Website die bestmögliche Verschlüsselung enthalten. Verschlüsselung ist, wie bereits erwähnt, ein Prozess, bei dem Daten in einen Code umgewandelt werden, der bei unbefugtem Zugriff nicht entziffert werden kann. Je besser die Verschlüsselung ist, desto schwerer ist es, die Online-Kommunikation zu verfolgen. Dies ist besonders wichtig, wenn Sie irgendeine Form von Online-Zahlung akzeptieren, eine Verbindung zu einem Bank- oder Maklerkonto herstellen, Krankendaten übertragen, die Datenschutz- und Sicherheitsstandards einer Regierungs- oder einer anderen Aufsichtsbehörde erfüllen müssen oder potenziell sensible Daten verarbeiten.

Branchenexperten empfehlen, für alle sicheren Online-Sitzungen mindestens eine 128-Bit-Verschlüsselung zu verwenden. Die Konfigurationen einiger Webserver und Client-Browser erlauben Sitzungen mit bis zu 256-Bit-Verschlüsselungsschutz, der höchsten Verschlüsselungsstufe, die derzeit kommerziell erhältlich ist. Welche Verschlüsselungsstufe für Sitzungen verfügbar ist, hängt davon ab, was der Browser und das Betriebssystem Ihres Kunden sowie Ihre eigenen Host-Serversysteme unterstützen. Wenn der Browser und das Betriebssystem Ihres Kunden keine höhere Verschlüsselungsstufe unterstützen, wird für die Sitzung automatisch die höchste Verschlüsselungsstufe gewählt, die unterstützt werden kann.

Viele Jahre lang galten in den USA Exportbeschränkungen für Browser, die die Hersteller daran hinderten, Produkte zu vertreiben, die höhere Verschlüsselungsstufen unterstützen. Obwohl die meisten Exportbeschränkungen im Januar 2000 aufgehoben wurden, gibt es viele Kunden, besonders außerhalb der USA, die immer noch ältere Browser (z. B. vor Microsoft Internet Explorer 5.5 (Export)) und Betriebssysteme (z. B. bestimmte frühe Windows 2000-Systeme) verwenden, bei denen automatisch die schwächeren, niedrigeren Verschlüsselungsstufen verwendet werden. Laut einer Schätzung der Yankee Group aus dem Jahr 2005 stellen viele Millionen von Internetbenutzern ihre Internetverbindungen mit unter der Norm liegenden Verschlüsselungsstufen her.[1]

SGC ist eine SSL-Erweiterung, die ursprünglich für Finanzinstitute geschaffen wurde, die von den US-amerikanischen Exportbeschränkungen für Verschlüsselung befreit waren. Bei SGC wird die Verschlüsselungsstufe vom Server gesteuert und hängt nicht vom Clientsystem ab. Nachdem die ursprünglichen Exportbeschränkungen aufgehoben wurden, werden nun SGC-aktivierte SSL-Zertifikate an alle Arten von Websites ausgegeben, nicht nur an autorisierte Finanzinstitute, wie in den späten 1990ern.

VeriSign bietet marktführende SGC-aktivierte SSL-Zertifikate, sodass praktisch jeder Besucher Ihrer Website durch die empfohlene 128-Bit-Mindestverschlüsselung geschützt ist.

1 2005, Yankee Group, Die Bausteine transparenter Websicherheit: Server-Gated Cryptography

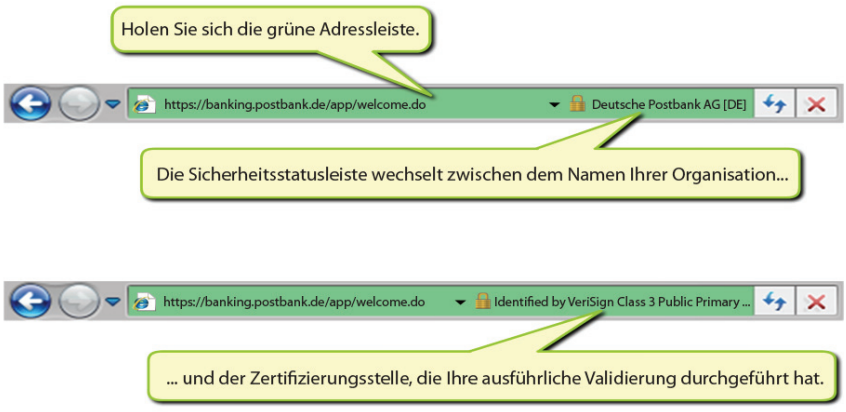
+ Extended Validation SSL (EV SSL): Höchste Sicherheit bei der Authentifizierung

Während immer mehr Menschen das Internet ohne Bedenken zur Informationssuche nutzen, ist die Zahl der Surfer doch erheblich größer als die Zahl derer, die das Internet für Online-Geschäfte nutzen. Laut einer Gartner-Umfrage von 2006 führten Sicherheitsbedenken dazu, dass beinahe die Hälfte aller Online-Kunden ihr Internetverhalten geändert haben, was die Online-Geschäftswelt fast 2 Milliarden Dollar gekostet hat.[2] Ganz offensichtlich bleiben zu viele potenzielle E-Commerce-Kunden misstrauisch oder haben Angst, einem unsichtbaren und nicht persönlich bekannten Gegenüber persönliche oder finanzielle Informationen preiszugeben. Sie benötigen eine Absicherung und verlangen diese auch immer häufiger, bevor sie persönliche Daten angeben oder eine finanzielle Transaktion abschließen.

Diese und ähnliche Beobachtungen führten dazu, dass eine Gruppe von Zertifizierungsstellen, Browser-Anbietern und WebTrust-Prüfern das CA/Browser Forum ins Leben gerufen hat, um einen neuen SSL-Standard zu entwickeln, den Online-Kunden problemlos verstehen und anwenden können. Dieses Konsortium, in dem unter anderem Repräsentanten von Microsoft und VeriSign vertreten sind, entwickelte Extended Validation (EV) SSL. Mit diesem neuen Standard soll die wachsende Zahl der Bedrohungen aus dem Internet, z. B. Phishing-Angriffe, bekämpft werden. Bei EV SSL müssen Websites einen strengen Authentifizierungsprozess durchlaufen. EV SSL gilt daher in der E-Commerce-Branche als höchster Standard für die Authentifizierung der legitimen Identität einer Website. Um EV SSL-Zertifikate ausgeben zu können, muss die Zertifizierungsstelle eine strenge WebTrust-Prüfung bestehen. VeriSign nimmt weiterhin eine Vorreiterrolle in der Entwicklung und der Implementierung dieses neuen Standards ein.

Ein EV SSL-Zertifikat bietet Online-Händlern und Online-Kunden ein weithin anerkanntes und empfohlenes Maß an Schutz vor immer raffinierteren Internet-Spoofing-Betrügereien. EV SSL bietet einige Verbesserungen der Benutzeroberfläche, damit Endkunden die Identifikation einer authentifizierten Site sofort deutlich erkennen können.

Neue, hochsichere Browser zeigen EV SSL-Zertifikate anders als herkömmliche SSL-Zertifikate an. Im Gegensatz zu den altbekannten SSL-Zertifikaten, bei denen ein unauffälliges Schlosssymbol angezeigt wird, wechselt bei EV SSL-Zertifikaten die Farbe der Adressleiste in hochsicheren Browsern und wird in einem auffälligen Grün angezeigt. Dieser Wechsel fällt Endkunden sofort ins Auge und schafft dadurch unmittelbar Vertrauen. Bei Overstock.com fiel auf, dass nach der Implementierung der EV SSL-Zertifikate von VeriSign die Besucher, die Microsoft® Internet Explorer 7 verwenden, durchschnittlich 8,6% mehr Transaktionen abschlossen als diejenigen, die alte, nicht-EV-fähige Browser verwenden. Nach der Bereitstellung von VeriSign EV SSL beobachtete DebtHelp.com sogar einen 11-prozentigen Anstieg der von Internet Explorer 7-Benutzern abgeschlossenen Transaktionen über ihre Website.



2 2006, Gartner, Trends in Consumer Society

Neben der auffälligen grünen Farbe zeigt eine Sicherheitsstatusleiste den Namen des Website-Besitzers und die Zertifizierungsstelle an, die das EV SSL-Zertifikat ausgestellt hat. Dort werden beide Namen abwechselnd angezeigt, wenn ein Besucher die Website zum ersten Mal aufruft.

Wie seine herkömmlichen SSL-Vorgänger ermöglicht auch das EV SSL-Zertifikat die sichere, verschlüsselte Kommunikation zwischen einer Website und dem Browser eines Kunden. Außerdem wird die Echtheit der Website authentifiziert, damit alle Besucher sicher sein können, dass sie tatsächlich die gewünschte Webseite aufgerufen haben und nicht auf eine gefälschte Webseite umgeleitet wurden.

Mit SSL-Zertifikaten von VeriSign profitieren Sie von einer hocheffektiven Authentifizierung sowie dem umfassenden Schutz der SGC-Verschlüsselung. VeriSign bietet Zertifikate an, die beide SSL-Weiterentwicklungen kombinieren.

+ Browser-Unterstützung für EV SSL

Microsoft hat, als erster Browserhersteller, der diesen neuen Standard unterstützt, die erweiterte EV SSL-Benutzeroberfläche in Microsoft Internet Explorer 7 integriert. Obwohl Microsoft Internet Explorer 7 noch nicht lange auf dem Markt ist, hat er doch bereits 31% des Browsermarkts erobert. Darüber hinaus können Benutzer von Firefox 2.0 eine Erweiterung herunterladen, die die Anzeige der grünen Adressleiste ermöglicht, wenn sie ein EV SSL-Zertifikat von VeriSign vorfinden. Diese Erweiterung wurde innerhalb eines Monats nach der Veröffentlichung bereits von mehr als 55.000 Firefox-Benutzern heruntergeladen. Gegenwärtig (im August 2007) bietet keine andere Zertifizierungsstelle diese Leistung an.

+ Vertrauensgütesiegel von Drittanbietern: Stärkung des Kundenvertrauens

So gut wie alle Käufer geben an, dass sie vor Identitätsdiebstahl, Kreditkartenbetrug und anderen Internet-Betrügereien Angst haben. Und sie haben jeden Grund dazu. Die finanziellen Verluste infolge von Identitätsdiebstahl beliefen sich allein von Juli 2005 bis Juli 2006 auf insgesamt 56,6 Milliarden US-Dollar, die durchschnittlichen Kosten pro Betrugsfall betrugen 6.383 US-Dollar.[4]

Neuerdings steigt bei den Verbrauchern das Bewusstsein für die Notwendigkeit von Lösungen zur Bekämpfung der Sicherheitsrisiken, für die sich sowohl die Internetsicherheitsbranche als auch bestimmte Regierungsbehörden stark einsetzen. Und ganz offensichtlich beschäftigen sich Online-Kunden immer intensiver mit dem Thema Internetsicherheit. Viele *erwarten* geradezu ein bekanntes Vertrauensgütesiegel eines Drittanbieters, das die Website des Online-Händlers als sichere und seriöse Einkaufsmöglichkeit ausweist. Die Integration eines etablierten Vertrauensgütesiegels von einem Drittanbieter auf der eigenen Website ist mittlerweile entscheidend wichtig, um „Surfer“ tatsächlich auch als Kunden zu gewinnen.

Studien haben ergeben, dass die Mehrheit der Online-Einkäufer das VeriSign Secured Seal™ erkennt und sich aufgrund dieses Siegels zum Online-Einkauf entscheiden würde.[5] Wenn Sie ein SSL-Zertifikat von VeriSign für Ihre Website erwerben, sind Sie dazu berechtigt, das exklusive VeriSign Secured Seal auf der Website anzuzeigen. Aufgrund dieses Siegels steigt das Vertrauen der Kunden in Ihre Website und damit auch die Zahl der abgeschlossenen Transaktionen. Außerdem können die Besucher auf das Siegel klicken, um Ihre Site zu überprüfen. Eine Woche nach der Integration des VeriSign Secured Seals auf der Website erlebte Opodo, ein führender paneuropäischer Reiseanbieter, einen Anstieg der Verkaufsabschlüsse um 10 Prozent.[6]

3. Mai 2007, www.marketshare.com
4 2006, Javelin Strategy/Better Business Bureau, Umfrage zu Identitätsbetrug
5 2006, Tech-Ed-Studie
6 Warren Jonas, Head of Services Management, Opodo

Nachdem Sie Ihre Website mit einem SSL-Zertifikat von VeriSign abgesichert haben, können Sie das Gütesiegel VeriSign Secured Seal einfach herunterladen und installieren.

+ Zusammenfassung

In der Welt der Internetsicherheit spielt Glaubwürdigkeit eine entscheidende Rolle. 88% der Internetnutzer erkennen VeriSign sofort[7], somit ist VeriSign derzeit die mit Abstand bekannteste SSL-Sicherheitsmarke der Welt. Diese Führungsposition konnte VeriSign erlangen, indem sich das Unternehmen aktiv an der Erarbeitung von Standards, der Weiterentwicklung von Protokollen und der Anwendung neuester Technologien für die Internetgemeinde beteiligt hat. Erfahrene Online-Kunden vertrauen der Marke VeriSign und fühlen sich sicher, wenn sie auf Websites einkaufen, die durch ein SSL-Zertifikat von VeriSign geschützt sind. Natürlich haben wir diesen Ruf nicht über Nacht erworben. Er gründet sich auf einer Vertrauensbasis, die seit Jahren gepflegt und durch das langjährige Engagement des Unternehmens und die Unterstützung bei der Entwicklung der Sicherheitsinfrastruktur des Internets immer wieder gestärkt wird.

Unternehmen, die auf Online-Transaktionen angewiesen sind, haben längst erkannt, dass eine zuverlässige und sichere Internetverbindung für die Rentabilität eines Unternehmens unverzichtbar ist. Je sicherer sich die Online-Kunden fühlen, desto erfolgreicher wird das Online-Unternehmen bei Aufbau und Bindung eines lukrativen Kundenstamms sein. Um ein Online-Unternehmen erfolgreich zu etablieren, müssen vertrauenswürdige Beziehungen zu allen potenziellen Kunden aufgebaut und gepflegt werden. Die Produkte von VeriSign tragen in hohem Maße zur Entwicklung solcher Beziehungen bei. Wenn Ihnen der Schutz und die Sicherheit potenziell vertraulicher Daten ein wichtiges Anliegen ist und Ihre potenziellen Kunden sicher sein sollen, dass Ihr Unternehmen ihre privaten Angaben respektiert und schützt, dann ist ein SSL-Zertifikat von VeriSign genau das Richtige für Sie.

Die Anzeige der Marke VeriSign auf Ihrer Website vermittelt Ihren potenziellen Kunden Seriosität und Vertrauenswürdigkeit. Ihre Kunden können sich beim Abschluss der Transaktion, die sie überhaupt erst zu Ihrer Site geführt hat, absolut sicher fühlen.

+ Über VeriSign

VeriSign unterhält die digitale Infrastruktur, die täglich Milliarden von Interaktionen über die weltweiten Sprach-, Video- und Datennetze ermöglicht und schützt.

Weitere Informationen finden Sie auf unserer Website www.VeriSign.de.

7 2006, Tech-Ed-Studie

00025049 08-29-07
ST 47149