



# VERTRAUEN ALS UNTERNEHMENSWERT

WIE SIE ALS UNTERNEHMEN DAS VERTRAUEN IHRER KUNDEN  
STÄRKEN UND IHREN ONLINE-UMSATZ STEIGERN KÖNNEN





# VERTRAUEN ALS UNTERNEHMENSWERT

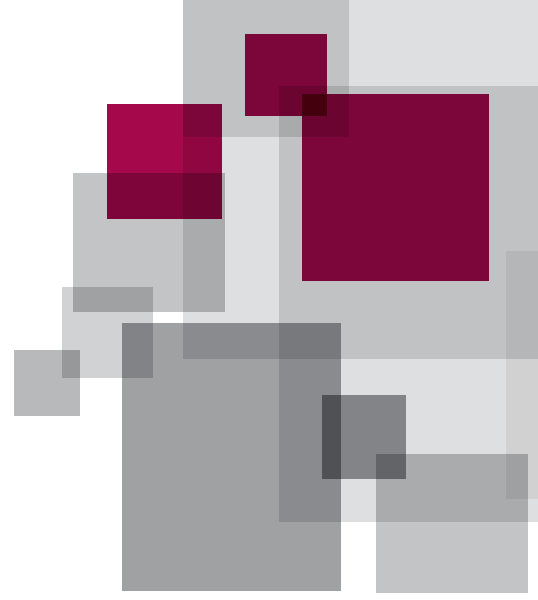
Möchten Sie Ihre Verkaufszahlen und Ihren Umsatz steigern? Sind Sie es leid, dass Internetnutzer zwar auf Ihrer Webseite stöbern, aber dann doch nichts kaufen? Alles eine Frage des Kundenvertrauens, findet VeriSign. Was IT-Verantwortliche unternehmen, damit die Kunden sich auf den Webseiten ihrer Unternehmen sicherer fühlen, erfahren Sie hier.

Der Betrieb einer E-Commerce-Webseite ist kein Kinderspiel. Angebot, Präsentation und Funktionen müssen stets topaktuell sein. Nicht minder wichtig ist der reibungslose und durchgängige Betrieb des E-Shops. Hier ein Patch einspielen, dort ein Problem beheben – es gibt immer etwas zu tun. Aber haben Sie dafür Ihre Webseite eingerichtet? Klare Antwort: Nein, Sie wollen darüber Ihre Produkte verkaufen.

Onlinenutzer kaufen eher bei E-Shops ein, denen sie vertrauen. Für 80 Prozent der von VeriSign befragten IT-Manager ist Vertrauensstärkung ein äußerst wichtiger Aspekt. Dennoch machen viele Händler im Internet auch von einfachen, zuverlässigen und erschwinglichen Mechanismen zur Vertrauensbildung keinen Gebrauch!

Dieser Bericht erläutert, wie wichtig Vertrauensstärkung für den E-Commerce ist, und welche Maßnahmen hierzu ergriffen (oder unterlassen) werden. Sie erfahren außerdem, wie Sie mit Unterstützung von VeriSign zügig und kostengünstig erreichen, dass u. U. mehr Besucher auf Ihrer Webseite einkaufen.





# WARUM VERTRAUEN WICHTIG IST

65 %

der Europäer den Verlust persönlicher Daten über das Internet<sup>iii</sup>.

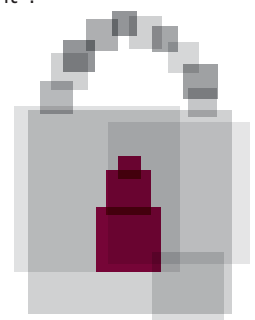
Vertrauen ist entscheidend, weil viele Onlinenutzer schlechte Erfahrungen gemacht haben. Nach Aussagen der Organisation Get Safe Online wurde 2008 in Großbritannien ein Drittel der Bevölkerung Opfer von Viren, ein Fünftel von Phishing und ein weiteres Fünftel von Identitätsdiebstahl. Mit der Folge, dass ein Drittel der Internetnutzer aus Sicherheitsbedenken oder mangelndem Vertrauen in die E-Händler gar nicht erst online einkauft<sup>i</sup>.

Die Zahl der tatsächlichen Opfer eines Internetbetrugs wird um ein Vielfaches übertroffen von der Zahl der Menschen, die Angst davor haben. Einer neueren Studie zufolge befürchten 65 Prozent der Europäer den Verlust persönlicher Daten über das Internet<sup>iii</sup>. Um solche Ängste wirksam zu zerstreuen, muss Ihre Webseite dem Besucher klar und deutlich vermitteln, dass er dort sicher ist<sup>iv</sup>.

Die gute Nachricht: Internetkäufer kennen sich in Sachen Onlinesicherheit immer besser aus. VeriSign-Umfragen zufolge weiß die überwiegende Mehrheit mit Webseite-Sicherheitsfunktionen wie dem HTTPS-Protokoll, dem

Vorhängeschloss, der grünen Adressleiste im Browser oder Internet-Gütesiegeln wie VeriSign Secured<sup>®</sup> etwas anzufangen. Abgelaufene Zertifikate hingegen wirken nicht vertrauenerweckend. Internetnutzer informieren sich darüber hinaus auch über mögliche Selbstschutzmaßnahmen und vergewissern sich, dass Datenschutz und Sicherheit auf der besuchten Webseite ernst genommen werden. Und sie kaufen eher nicht auf Seiten ein, auf denen das nicht der Fall ist.

Sie sehen, es steht einiges auf dem Spiel. 2011 wird der E-Commerce-Umsatz in Europa ein Volumen von bis zu 275 Milliarden GBP haben<sup>v</sup> und 70 Prozent der britischen Verbraucher kaufen bereits im Internet ein<sup>vi</sup>. In Spitzenzeiten wie dem Weihnachtsgeschäft werden sogar Werte bis zu 93 Prozent erreicht<sup>vi</sup>.





# IMMER MEHR GEFAHREN FÜR DEN E-COMMERCE

Die Bedenken der Käufer sind leider berechtigt: Cyberverbrecher sind kreativ und hochmotiviert. Internetkriminalität ist ein wesentlich gewinnbringenderes Geschäft als der Drogenhandel und darüber hinaus für die Täter risikoärmer. Es handelt sich um eine ausgeklügelte Schattenwirtschaft, in der dauernd neue und immer speziellere Taktiken angewendet werden. Hacker verkaufen ihre Programme und ihr Know-how an Mittelsmänner, die ihrerseits den Verkauf von Hehlerware oder Geldwäsche und Kreditkartenfälschung organisieren.

Kurzum, Cyberverbrechen ist ein wachsendes Problem. APACS zufolge nahmen zwischen 2007 und 2008 der Internet- und der Telefonkartenbetrug um 13 Prozent zu. In der ersten Hälfte des Jahres 2009 lag der Schaden in Großbritannien bei 134 Millionen GBP<sup>viii</sup> und hat sich damit seit 2000 verdreifacht. Das Umsatzvolumen des E-Commerce verdoppelte sich im gleichen Zeitraum lediglich<sup>ix</sup>.

Doch das Risiko im Internet beschränkt sich nicht nur auf Verbraucher. Auch Unternehmen müssen sich mit Hackern, Webseite-Fälschungen, der Lahmlegung von Systemen und Diensten, mit Spyware und Datendiebstahl herumschlagen. Die neueste Studie zu Sicherheitsverletzungen des britischen Wirtschaftsministeriums<sup>x</sup> ergab, dass im Jahr 2008 45 Prozent der Kleinunternehmen Schäden durch Cyberkriminalität in Höhe von 10.000 bis 20.000 GBP zu verkraften hatten. Noch stärker betroffen waren große Unternehmen (72 Prozent), mit wesentlich gravierenderen Schäden von durchschnittlich 90.000 bis 170.000 GBP. Zwei Internetgefahren – Datendiebstahl und Webseite-Fälschung – unterminieren das Vertrauen der Kunden drastisch. Wer sich hier einen Fehler leistet, setzt seinen guten Ruf aufs Spiel.

Diese Ansicht wird von den für diesen Bericht Befragten geteilt. Sie nahmen die Befürchtungen der Kunden sehr ernst (71 Prozent). Ein Großteil stufte die folgenden Risiken als „sehr bedeutend“ ein:

- Webseite-Fälschung (44 Prozent)
- Phishing (40 Prozent)
- Identitätsdiebstahl (63 Prozent)

Genannt wird auch der Punkt Zertifikatsverwaltung sowie die damit verbundenen Risiken, etwa wenn Zertifikate auslaufen oder ihr Inhalt nicht aktuell gehalten wird. 36 Prozent der Befragten fanden die Verwaltung mehrerer Zertifikate problematisch und für 53 Prozent war das unerwartete Ablaufen von Zertifikaten ein Thema.

In anderen Worten: Es gibt reale Probleme, und sowohl IT-Manager als auch Verbraucher stufen sie als Hindernis für den E-Commerce ein. Gut also, dass es einfache, problemlos verfügbare und zuverlässige Methoden gibt, mit denen Sie das Vertrauen Ihrer Kunden stärken und ihre Daten schützen können.



**45 %**

Prozent der Kleinunternehmen Schäden durch Cyberkriminalität.

# VERISIGN- LÖSUNGEN



Mit VeriSign schlagen Sie gleich zwei Fliegen mit einer Klappe: Erstens schützen Sie damit Ihre Kunden durch Verschlüsselung ihrer persönlichen Daten und Schaffung einer sicheren Webseite-Umgebung. Zweitens bringen Sie damit klar ersichtlich zum Ausdruck, dass

Ihnen der Schutz und die Sicherheit von Kundendaten am Herzen liegen. Unsere Befragung ermittelte einzelne E-Commerce-Geschäftsziele, und VeriSign stellt die Technik für ihre Umsetzung bereit.

Geschäftsziel	Eingestuft als „sehr wichtig“ von	VeriSign-Lösungen
Förderung des Kundenvertrauens	80 Prozent	Angesichts der vielen Anbieter von SSL-Zertifikaten ist die Auswahl eines Anbieters sinnvoll, der für größtmögliches Vertrauen bei Internetkäufern sorgt. Neuen Untersuchungen zufolge ist das VeriSign-Secured-Siegel in Großbritannien 81 Prozent der Onlinekäufer bekannt – ein Wert, den kein anderes Siegel erreicht <sup>xi</sup> – und europaweit assoziieren 78 Prozent der Onlinekäufer den Namen VeriSign am ehesten mit der Eigenschaft <i>vertrauenswürdig</i> <sup>xii</sup> . Mit dem VeriSign-Secured-Siegel können Ihre Webseite-Besucher die Gültigkeit des SSL-Zertifikats prüfen und haben einen sichtbaren Beweis dafür, dass Sie ihre Daten durch einen vertrauenswürdigen Anbieter schützen lassen. Ähnlich verhält es sich mit SSL-Zertifikaten mit erweiterter Prüfung: Sie zeigen den Namen des Webseite-Eigentümers an und hinterlegen in modernen Browsern die Adressleiste grün – ein klares Zeichen dafür, dass die Seite echt und die SSL-Verschlüsselung aktiv ist.
Mehr Sicherheit	64 Prozent	VeriSign Server Gated Cryptography (SGC) ermöglicht je nach Browser, Betriebssystem und Host-Server die Verschlüsselung mit 128 oder 256 Bit und ist damit die leistungsfähigste Verschlüsselung, die heute auf dem kommerziellen Markt erhältlich ist. Mehr als 99,9 % der Webseitebesucher werden mit VeriSign SGC geschützt. <sup>xiii</sup> Ergebnis: Die Kundendaten bleiben bei der Übertragung zwischen Browser und Server auf jeden Fall sicher.
Höherer Markenwert	54 Prozent	Die überwiegende Mehrheit (84 Prozent) der britischen Internetkäufer kennt Webseite-Sicherheitsfunktionen wie das HTTPS-Protokoll, das Vorhängeschloss, die grüne Adressleiste im Browser oder Internet-Gütesiegel. <sup>xiv</sup> Mit diesen visuellen Hinweisen können Sie also wunderbar die Vertrauenswürdigkeit Ihrer Marke und Ihrer Webseite herausstreichen. Mit dem VeriSign® Certificate Center oder VeriSign® Managed PKI für SSL (für größere Unternehmen) bietet VeriSign Ihnen außerdem eine einheitliche Zertifikatsverwaltung. So laufen Zertifikate nicht mehr unbemerkt ab und Sie riskieren weder Sicherheitslücken noch potenzielle Rufschädigungen.
Höhere Abschlussraten	44 Prozent	Besucher auf Ihre Webseite zu locken, ist eine Sache. Aber sie sollten dort natürlich auch einkaufen. Die Besuchszahlen können Sie mühelos mit den richtigen Marketingmaßnahmen steigern. Entscheidend für das Zustandekommen eines Geschäfts ist jedoch das Geschehen auf der Seite selbst. Über zwei Drittel der Befragten (68 Prozent) gaben an, bei Online-Anbietern ohne erkennbares Gütesiegel oder sonstige Sicherheitsnachweise nur ungern einzukaufen. <sup>xv</sup> Durch die Verwendung von SSL-Zertifikaten mit erweiterter Prüfung und Gütesiegeln wie VeriSign Secured fühlen sich Onlinekäufer beim Durchsuchen des Angebots und der Eingabe persönlicher Daten sicher. Noch seriöser wirkt es außerdem, wenn Sie Ihre Käufer darüber informieren, was Sie zu ihrem Schutz auf Ihrer Webseite unternehmen.
Höherer Auftragsumfang	34 Prozent	Ein hohes Maß an Vertrauen und Sicherheit fördert auch den Verkauf ergänzender Produkte und Dienstleistungen. Auf wenig seriös wirkenden Webseiten werden Links zu Garantieverlängerungen oder ähnlichen Produkten eher als Spam oder lästige Popup-Werbung wahrgenommen. Umgekehrt gilt: Auf vertrauenerweckenden Seiten werden derlei Angebote oft genauer studiert. Insbesondere gilt dies, wenn die Besucher Ihrer Webseite Daten eingeben müssen. So benötigt beispielsweise ein Versicherungsanbieter vorab eine Menge persönlicher Angaben, um dem Kunden ein Angebot unterbreiten zu können. Die Erfahrung zeigt, dass mit steigendem Unsicherheitsgefühl der Kunden auf einer Webseite die Einkaufsabbrüche zunehmen und die Anmeldearten sinken.





# WIE UNTERNEHMEN SICH SCHÜTZEN

Eine aufgeklärte Mehrheit der E-Commerce-Händler beherzigt unsere Tipps bereits: den Einsatz von SSL-Zertifikaten mit erweiterter Prüfung, das Einblenden von Gütesiegeln wie dem VeriSign-Secured-Siegel und deutliche visuelle Hinweise zu den für die Webseite geltenden Sicherheitsmaßnahmen. Erstaunlicherweise ignorieren aber genügend Unternehmen die guten Ratschläge immer noch. Nur 40 Prozent der von uns Befragten verwenden die erweiterte Gültigkeitsprüfung; nur 32 Prozent machen Gebrauch von Gütesiegeln. Außerdem gibt es bei nur 30 Prozent eine zentrale Zertifikatsverwaltung.

Warum riskieren, dass die Kunden zur Konkurrenz gehen, die vielleicht geschickter ist? Die Maßnahmen sind schlicht und ergreifend ein Wettbewerbsvorteil.

Und was müssen Sie unternehmen? Eigentlich nicht viel. Die Einrichtung ist kein Hexenwerk und erschwinglich dazu. Der Umstieg von einem regulären SSL-Zertifikat auf ein Extended Validation SSL-Zertifikat ist technisch einfach, und VeriSign kann Sie dabei unterstützen. Ein Gütesiegel und Erläuterungen zum Thema Onlinesicherheit lassen sich ohne Aufwand dezent in Ihre Webseite integrieren. Und mit einer zentralen Zertifikatsverwaltung stellen Sie sicher, dass Ihre Zertifikate nicht unbemerkt ablaufen.

**Tabelle: Vertrauensbildende Maßnahmen**

SSL-Zertifikate	84 %
SSL-Zertifikate mit erweiterter Prüfung	40 %
Gütesiegel (z. B. VeriSign Secured)	32 %
Hinweis auf Sicherheitsfunktionen	25 %

Quelle: VeriSign-Befragung IT-Manager Januar 2010

# EMPFEHLUNGEN VON VERISIGN

VeriSign-Kunden berichten, dass nach dem Ergreifen der Schutzmaßnahmen ihre Abschlussraten und der Umsatz enorm anstiegen und Einkaufsabbrüche abnahmen. Bei Misco waren es nach der Einführung von Extended Validation SSL-Zertifikaten beispielsweise fünf Prozent weniger Einkaufsabbrüche.\* Directline Holidays verzeichnete eine acht Prozent höhere Abschlussrate.\* Bei QuickRooms.com kam es nach Einführung von SSL-Zertifikaten mit erweiterter Prüfung zu einer Umsatzsteigerung von fast sieben Prozent.\*

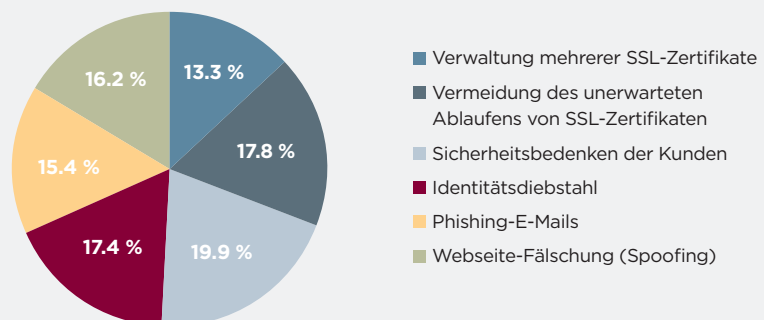
Sicher waren bei den genannten Unternehmen noch andere Faktoren im Spiel und die Zahlen

werden bei Ihnen keinesfalls exakt gleich ausfallen, dennoch: Gemessen an einem durchschnittlichen Webseitenumsatz-Budget müssen Sie relativ wenig investieren, der potenzielle Gewinnzuwachs im Gegenzug ist relativ hoch. Eine solche Investition spricht für sich selbst.

Sie profitieren außerdem auch langfristig: In einem ständig wachsenden Markt mit immer schärferem Wettbewerb heben Sie sich mit Vertrauensbildung ab und können Abschlussraten und Auftragsvolumina steigern. Der Schritt ist also nicht nur eine Frage der Vernunft, Ihr Geschäft wird davon profitieren.

Die Sicherheitsbedenken ihrer Kunden standen für IT-Manager an erster Stelle.

„Wie wichtig sind Ihnen die folgenden Themen?“



# VERISIGN

VeriSign (NASDAQ: VRSN) ist führender Anbieter von Internet-Infrastrukturdiensten für die vernetzte Welt. Milliardenfach pro Tag unterstützt VeriSign mit SSL, Authentifizierung, Identitätsschutz und Registrierungsservices Unternehmen und Kunden weltweit bei vertrauensvoller Kommunikation und sicherem Handel.

VeriSign ist eine führende SSL-Zertifizierungsstelle (Secure Sockets Layer) und verwandelt Webseiten, Intranets und Extranets in eine sichere Umgebung, in der Ihre Kunden vollkommen vertraulich mit Ihnen interagieren und Geschäfte tätigen können. VeriSign ist führender SSL-Zertifikatsanbieter und ein Mitglied des CA/Browser Forum, eines freiwilligen Zusammenschlusses von EV-SSL-Zertifizierungsstellen und Browserherstellern.

➤ Weitere Informationen erhalten Sie unter **www.verisign.de**

<sup>i</sup> VeriSign-Befragung vom 4.-13. Januar 2010

<sup>ii</sup> „Angst hält vom Onlinekauf ab“ BBC-Nachrichten, Mai 2009. Verfügbar unter <http://news.bbc.co.uk/2/hi/business/8043717.stm>

<sup>iii</sup> „EU-Experten: Datenverlust ist ein europaweites Problem“ SC Magazine, Oktober 2008. Verfügbar unter <http://www.scmagazineuk.com/Data-loss-is-Europe-wide-problem-says-EU-expert/article/119969/>

<sup>iv</sup> Get Safe Online: GSO Jahresbericht 2009, [www.getsafeonline.org](http://www.getsafeonline.org)

<sup>v</sup> Bericht von eMarketer, Mai 2008

<sup>vi</sup> Get Safe Online: GSO Jahresbericht 2009, [www.getsafeonline.org](http://www.getsafeonline.org)

<sup>vii</sup> IMRG Research: <http://www.imrg.org>

<sup>viii</sup> APACS: [http://www.ukpayments.org.uk/media\\_centre/press\\_releases/-/page/732/](http://www.ukpayments.org.uk/media_centre/press_releases/-/page/732/)

<sup>ix</sup> APACS: [http://www.ukpayments.org.uk/resources\\_publications/key\\_facts\\_and\\_figures/card\\_fraud\\_facts\\_and\\_figures/](http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/)

<sup>x</sup> Department for Business, Innovation and Skills: Studie zu Sicherheitsverletzungen: [http://www.pwc.co.uk/eng/publications/berr\\_information\\_security\\_breaches\\_survey\\_2008.html](http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html)

<sup>xi</sup> VeriSign 2009 Brand Research, Synovate/GMI, Mai 2009

<sup>xii</sup> Synovate/GMI, Ibid.

<sup>xiii</sup> SGC: <http://www.verisign.com/ssl/ssl-information-center/strongest-ssl-encryption/index.html>

<sup>xiv</sup> VeriSign 2009 Brand Research\* Synovate/GMI, May 2009

<sup>xv</sup> Synovate/GMI Ibid.

\* Ihre eigenen Ergebnisse fallen u. U. anders aus. Zu den dargestellten Ergebnissen tragen möglicherweise auch für die erwähnten Unternehmen spezifische Faktoren bei. VeriSign berät Sie gerne, was die Umsetzung Ihrer Sicherheitsanforderungen angeht.

© 2010 VeriSign SARL. Alle Rechte vorbehalten. VeriSign, das VeriSign-Logo, das Häkchen im Kreis und andere Marken, Dienstleistungsmarken und Designs sind eingetragene oder nicht eingetragene Marken von VeriSign und seinen Niederlassungen in den U.S.A. und anderen Ländern. Alle anderen Marken sind Eigentum der jeweiligen Inhaber.

