



# **KUNDEN GEWINNEN UND ONLINE VERTRAUEN AUFBAUEN – EIN LEITFADEN**

WIE KLUGE UNTERNEHMEN ONLINE  
VERTRAUEN SCHAFFEN UND ALS  
WETTBEWERBSVORTEIL NUTZEN

# ➤ KUNDEN GEWINNEN UND ONLINE VERTRAUEN AUFBAUEN - EIN LEITFADEN

Wie kluge Unternehmen online Vertrauen schaffen und als Wettbewerbsvorteil nutzen

34%

der Interbenutzer in Großbritannien waren bereits einmal Opfer eines Computervirus.<sup>1</sup>

Ein Unternehmen mit einer Webseite ist auf das Vertrauen seiner Kunden angewiesen. Es kostet viel Geld, eine gute Website zu erstellen. Es kostet noch mehr Geld, eine Marke aufzubauen und sie bekannt zu machen. Wer auf den letzten Metern potenzielle Kunden verliert, nur weil ihnen das Vertrauen zum Kauf fehlt, hat also eine Menge Geld in den Sand gesetzt. Schlimmer noch: er gefährdet den Geschäftserfolg. Die Situation ist vergleichbar mit einem Marathonläufer, der kurz vor der Ziellinie stehen bleibt.

## SUBJEKTIVES RISIKOEMPFINDEN

Zahlreiche Medienberichte über Sicherheitsprobleme im Internet verunsichern Verbraucher, was für Unternehmen deutliche Folgen hat: Einige potenzielle Kunden tätigen überhaupt keine Käufe online. Andere sind äußerst wählerisch, was ihre Geschäftspartner angeht, und machen einen Bogen um Websites, bei denen sie sich nicht sicher fühlen. Wiederum andere klicken sich bis zur Online-Kasse durch und brechen dann den Kauf ab, wenn sie das Gefühl haben, dass ihre persönlichen Daten nicht gut genug geschützt werden.

„Get Safe Online“, eine von VeriSign unterstützte Internet-Initiative der britischen Regierung, bietet aufschlussreiche Zahlen zur Bereitschaft der Briten Online-Geschäfte zu tätigen. Viele Kunden kaufen ohne Bedenken im Internet ein, verwalten ihr Bankkonto

online oder buchen ihren Urlaub im Netz – aber viele eben auch nicht. Ungefähr ein Drittel der britischen Bevölkerung vermeidet Online-Käufe: 34 Prozent der Interbenutzer in Großbritannien waren bereits einmal Opfer eines Computervirus. Andere weitverbreitete Online Verbrechen sind: Phishing (22 Prozent), Online-Betrug (15 Prozent) und Identitätsdiebstahl (21 Prozent)<sup>1</sup>.

## VERTRAUEN ALS WETTBEWERBSVORTEIL

Auf der Liste eines Verantwortlichen für E-Business stehen viele Ziele: weniger abgebrochene Einkaufsvorgänge, größere Auftragswerte, stabile Gewinnmargen, höhere Rendite bei Kosten für Werbemaßnahmen, besseres Abschneiden im Vergleich mit Branchengrößen – und der maßgebliche Faktor für das Gelingen ist Vertrauen. Wenn es um mehr als nur Online-Einkäufe geht, ist Vertrauen sogar noch wichtiger. So müssen Kunden bei Finanzgeschäften oder Versicherungen weit mehr Daten von sich preisgeben als beim Online-Versandhandel. Noch persönlicher wird es im Gesundheitswesen oder bei der Online-Steuererklärung: Ohne Vertrauen geht es hier nicht.

Wenn es Ihnen gelingt, Ihre Website vertrauenswürdiger zu machen, können Sie die Sorge um Sicherheit in Ihren Vorteil umwandeln: Vertrauen kann ein Wettbewerbsvorteil sein.

<sup>1</sup> „Get Safe Online“-Bericht 2009:  
[http://www.getsafeonline.org/nqcontent.cfm?a\\_id=1517](http://www.getsafeonline.org/nqcontent.cfm?a_id=1517).

# ECHE FIRMEN, HARTE FAKTEN

Wir wollten herausfinden, worüber man sich in Unternehmen Sorgen macht und was man zur Kundengewinnung und zur Schaffung von Vertrauen in die Online-Angebote unternimmt. Dazu haben wir 276 IT-Verantwortliche in Deutschland befragt.

Zunächst fragten wir, wovor die Kunden ihrer Meinung nach Angst haben. Dies liefert einen Hinweis auf die Bedrohungen, gegen die Unternehmen sich wappnen möchten.

Als größtes Risiko wurden finanzielle Verluste und Betrügereien eingeschätzt, dicht gefolgt von unseriösen Händlern. Offenbar spiegeln sich in diesen Zahlen die Medienberichte über Online-Kriminalität und die Ergebnisse von Benutzerumfragen wider. Hieraus folgt für IT-Verantwortliche, dass die nachweisliche Authentizität ihrer Website von besonderer Wichtigkeit ist, damit Kunden erkennen, dass ihre Kreditkartendaten sicher sind und nicht von Kriminellen abgefangen werden.

Dann fragten wir, was den IT-Managern selbst Sorgen bereitet, und hier präsentierte sich die Situation schon etwas anders. Die Fachleute waren weniger besorgt über Identitätsdiebstahl oder Phishing, sondern ihnen lag – verständlicherweise – vor allem am Herzen, dass ihre Kunden sich sicher fühlen. Aber auch praktische Erwägungen spielten eine große Rolle: So stand die Sorge, dass ein SSL-Zertifikat plötzlich ablaufen könnte, an zweiter Stelle.

Auch diese Sorgen sind nachvollziehbar. Die Fälschung von Websites ist eine reale Bedrohung: Allein im letzten Quartal des Jahres 2009 wurden über 900 Marken gekapert.<sup>2</sup> Phishing kann den Ruf einer Marke durch gefälschte E-Mails und Websites, die vorgeben, zu einer bekannten Marke zu gehören, zerstören. Aus diesen Fakten folgt eines: Der Nachweis, dass ihre Website authentisch und keine Fälschung ist, muss für Unternehmen oberste Priorität haben. Da das mangelnde öffentliche Vertrauen in Online-Geschäfte vor allem in der Angst vor Identitätsdiebstahl begründet ist,<sup>3</sup> müssen die Inhaber von Websites deutlich zu erkennen geben, dass persönliche Daten angemessen geschützt werden, beispielsweise durch eine verschlüsselte Übertragung.

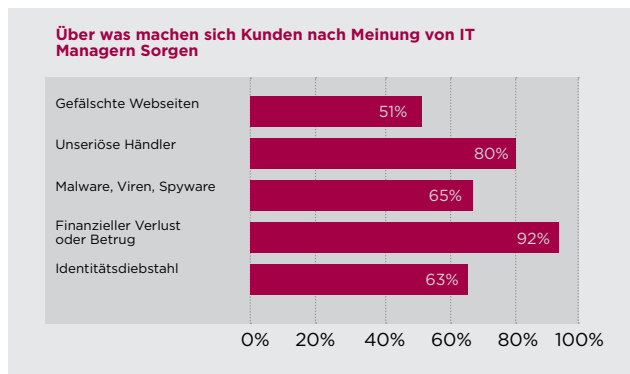
Abgelaufene SSL-Zertifikate können das Vertrauen erheblich schwächen, denn sie verursachen im Browser beunruhigende Fehlermeldungen (deren Fachjargon zudem nur schwer verständlich ist). Den Überblick über die Termine zur

Erneuerung von Zertifikaten verliert man schneller, als man annehmen würde, insbesondere wenn viele SSL-Zertifikate verwaltet werden müssen. Gefordert ist somit eine effiziente Verwaltung von Zertifikaten, die sicherstellt, dass sie nicht versehentlich ablaufen.

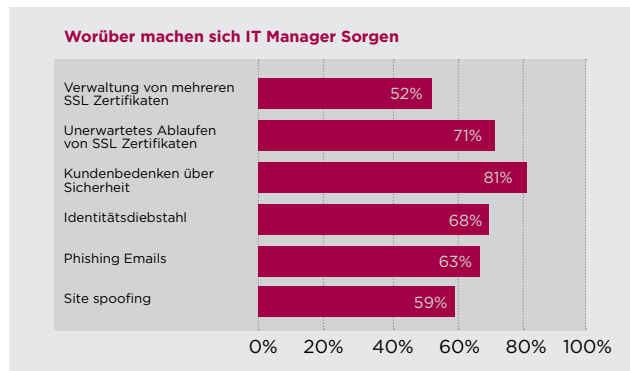
Weiterhin haben wir uns nach den Maßnahmen erkundigt, die die Teilnehmer unserer Umfrage zur Erhöhung von Vertrauen und Sicherheit ergreifen. Der eindeutige Spitzenreiter

waren hier SSL-Zertifikate zur Verschlüsselung vertraulicher Daten, allerdings nutzten erstaunlich wenige Teilnehmer die sicherste und sichtbarste Art von SSL-Zertifikaten, nämlich Extended Validation SSL-Zertifikate. Nur wenige verwendeten Vertrauenszeichen wie das VeriSign Secured<sup>®</sup> Seal, und noch weniger informierten die Website-Besucher über die verwendeten Schutzmechanismen, etwa auf einer eigenen Seite mit Sicherheitshinweisen. Offenbar gibt es viele Webmaster, die noch nicht alle Raffineszen kennen.

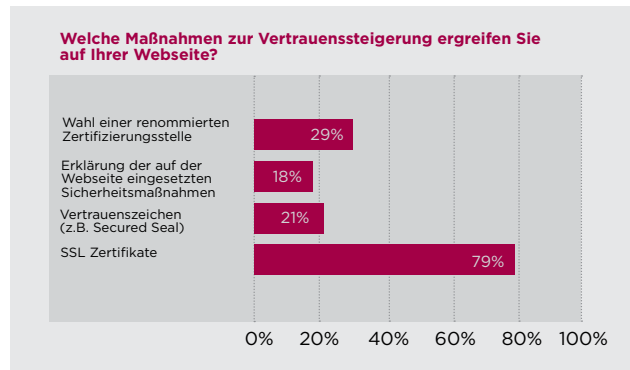
(i)



(ii)



(iii)



<sup>2</sup> Anti-Phishing Working Group, Dezember 2009, [www.apwg.org](http://www.apwg.org)

<sup>3</sup> Umfrage von Synovate und GMI, 2009



# VORTEILE VON EXTENDED VALIDATION SSL-ZERTIFIKATEN

Welche Bedeutung hat Vertrauen eigentlich? Zum Einen handelt es sich um eine Reaktion auf Online-Kriminalität wie etwa Identitätsdiebstahl. Zum Anderen geht es darum, das Sicherheitsbewusstsein der Kunden anzusprechen. Wir haben den Begriff „Vertrauen“ in vier Aspekte aufgeteilt:

- Authentifizierung des Verkäufers („Wir sind die, die wir vorgeben zu sein.“)
- Datenschutz und -verschlüsselung („Wir schützen Ihre Daten.“)
- Aufwertung der Marke („Wir respektieren Ihre Privatsphäre.“)
- Steigerung des Vertrauens („Sie können hier sicher einkaufen.“)

Extended Validation SSL-Zertifikate sind eine Verbesserung gegenüber herkömmlichen SSL-Zertifikaten, denn sie zeigen den Firmennamen an und hinterlegen die Adressleiste. Dies funktioniert bei bestimmten Browsern, z. B. Internet Explorer ab Version 7 oder Firefox ab Version 3.0, und bei den neuesten Smartphones. So erkennen die Kunden auf den ersten Blick, dass die Website vertrauenswürdig ist.

SSL-Zertifikate sprechen alle vier Aspekte an:

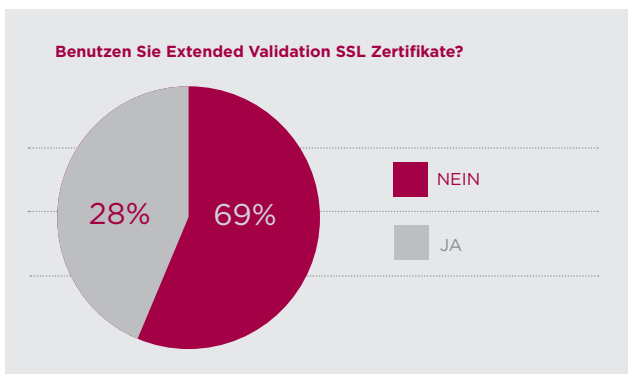
- **Authentifizierung des Verkäufers:** VeriSign vergibt Zertifikate erst nach einer Authentifizierung, für die strenge Vorschriften gelten. So können Website-Besucher sicher sein, dass die Website echt ist.
- **Datenschutz und -verschlüsselung:** SSL-Zertifikate mit EV verwenden für die verschlüsselte Übertragung der Benutzerdaten zwischen Browser und Server eine stärkere Verschlüsselung als herkömmliche SSL-Zertifikate.
- **Aufwertung der Marke:** SSL-Zertifikate mit EV zeigen den Firmennamen in der Adressleiste kompatibler Browser an. So erkennen Besucher, dass die Webseite tatsächlich zum erwarteten Unternehmen gehört.
- **Steigerung des Vertrauens:** Die grüne Adressleiste ist ein sichtbares und zuverlässiges Zeichen höchster Sicherheit für die Besucher von Websites, die durch SSL-Zertifikate mit EV geschützt werden.

## EXTENDED VALIDATION SSL-ZERTIFIKATE

Extended Validation SSL-Zertifikate sind die direkte Antwort auf die Zunahme von Betrugsfällen im Internet, die das Kundenvertrauen in Online-Transaktionen untergraben. Der Extended Validation SSL-Standard legt die Messlatte für die Überprüfung für SSL-Zertifikate höher und bietet optische Anzeigen in hochsicheren Webbrowsern.

2006 hat eine Gruppe aus führenden SSL-Zertifizierungsstellen (Certificate Authorities, CAs) und Browser-Anbietern Standards für die Genehmigung und Anzeige von Zertifikaten, den sogenannten Extended Validation-Standard, beschlossen. Für die Ausstellung eines SSL-Zertifikats, das diesen Standard erfüllt, muss die CA die Extended Validation-Verfahren übernehmen und ein WebTrust-Audit bestehen. Im Validierungsverfahren muss die CA sicherstellen, dass der Antragsteller für das Zertifikat der Eigentümer der Domain ist und die jeweilige genehmigende Person beim Antragsteller angestellt und befugt ist, Extended Validation SSL-Zertifikate zu erwerben. Zudem muss die Identität des Unternehmens überprüft werden.

Extended Validation SSL-Zertifikate bieten in hochsicheren Webbrowsern Informationen zur eindeutigen Identifizierung des Unternehmens, das hinter einer Website steht. Wenn Sie beispielsweise mit Microsoft® Internet Explorer 7 auf eine Website zugreifen, die mit einem SSL-Zertifikat geschützt ist, das den Extended Validation-Standard erfüllt, wird die URL-Adressleiste in IE7 grün hinterlegt. Neben der grünen Adressleiste wird ein Feld angezeigt, über das Sie den Namen der Organisation im Zertifikat oder die Zertifizierungsstelle (beispielsweise VeriSign) anzeigen können. Auch Firefox 3 unterstützt Extended Validation SSL.



# GREIFBARE RESULTATE

Unsere Umfrage ergab, dass Unternehmen, die SSL-Zertifikate mit EV einsetzen, greifbare Vorteile verzeichnen konnten: größere Auftragswerte, weniger abgebrochene Einkaufsvorgänge, höherer Umsatz. Das wertvollste Resultat war allerdings, dass Kunden die Sicherheit dieser Websites besser beurteilten, wie die deutliche Mehrheit von 62 Prozent der Befragten berichtete.

Tatsächlich stellen wir genau dies immer wieder bei unseren Kunden fest: Unternehmen, die ihre Websites mit VeriSign EV SSL-Zertifikaten schützen, melden durchschnittliche Steigerungen der Verkaufszahlen von über 20 Prozent.<sup>4</sup> Aktuelle Fallstudien von VeriSign-Kunden, die EV SSL-Zertifikate einsetzen, belegen eindrucksvolle Vorteile:<sup>\*</sup>

- Misco, ein Elektronik-Einzelhändler, verzeichnete fünf Prozent weniger Einkaufsabbrüche.
- Directline Holidays verzeichnete eine um acht Prozent höhere Abschlussrate.
- QuickRooms.com steigerte seinen Umsatz um fast sieben Prozent.
- Papercheck.com konnte seine Online-Anmeldungen fast verdoppeln (Steigerung um 87 Prozent).
- CarInsurance.com verzeichnete um 18 Prozent mehr Online-Abschlüsse.
- Fitness Footwear steigerte seine Abschlussrate um 16,9 Prozent und senkte die Einkaufsabbrüche um 13,3 Prozent.
- CreditKarma.com steigerte seine Abschlussrate um 26 Prozent.

## EMPFEHLUNGEN VON VERISIGN

Sie können das Vertrauen Ihrer Kunden mit fünf einfachen Schritten stärken:

- **Wechseln Sie zu EV SSL.** SSL ist gut, Extended Validation SSL ist besser. Extended Validation-Zertifikate ersetzen herkömmliche SSL-Zertifikate, kosten nur unwesentlich mehr und erfordern kaum Mehraufwand bei der Implementierung.

- **Entscheiden Sie sich für eine vertrauenswürdige Zertifizierungsstelle.** Benutzer legen großen Wert auf die Reputation der Zertifizierungsstelle (wie VeriSign). In einer Studie gaben 88 Prozent der Teilnehmer an, dass sie VeriSign vertrauten. Der zweitplatzierten Zertifizierungsstelle vertrauten dagegen nur noch 22 Prozent der Befragten.<sup>5</sup>
- **Verwenden Sie ein Vertrauenszeichen.** Verbessern Sie die Wirkung von SSL-Zertifikaten mit EV durch zusätzliche Erkennungsmerkmale, die zeigen, dass Sie Wert auf die Sicherheit Ihrer Kunden legen. Hierbei empfiehlt es sich, ein Vertrauenszeichen mit einem hohen Bekanntheitsgrad zu wählen. In Großbritannien beispielsweise wird das VeriSign Secured Seal von 81 Prozent der Online-Kunden erkannt, deutlich mehr als jedes andere Vertrauenszeichen.<sup>6</sup>
- **Verbessern Sie die Zertifikatverwaltung.** Eine Überwachung Ihrer Zertifikate kann gewährleisten, dass Sie vor dem Ablauf eines Zertifikats automatisch gewarnt werden. Überlegen Sie, ob es hilfreich wäre, alle Zertifikate in einem verwalteten Konto zusammenzulegen. Das VeriSign Certificate Center unterstützt Sie bei der zentralen Online-Verwaltung Ihrer VeriSign-Zertifikate. Wenn Sie zahlreiche Zertifikate oder Zertifikate von verschiedenen Zertifizierungsstellen nutzen, investieren Sie in ein Verwaltungstool wie VeriSign Managed PKI für SSL.

- **Erzählen Sie Ihren Kunden, was Sie für ihren Schutz tun.** Ihre Kunden wissen, woran sie sind, wenn sie in der Hilfe oder in der Fußzeile der Webseite erfahren, wie Sie für ihren Schutz sorgen. Dort können Sie auch beschreiben, wie ein SSL-Zertifikat funktioniert.

Bei den Teilnehmern an unseren Studien entfallen durchschnittlich 12 Prozent ihrer Ausgaben, und damit ein erheblicher Anteil an ihren Gesamtausgaben, auf Sicherheitsmaßnahmen. Und dennoch

trafen viele Unternehmen nicht einmal diese einfachen Maßnahmen, um Kundenvertrauen, Sicherheit und Vertrauenswürdigkeit ihrer Websites zu erhöhen.

Zugegeben, einen gewissen Zeitaufwand erfordern diese Maßnahmen durchaus (beispielsweise für eine Änderung des Seitendesigns, um das Vertrauenszeichen auf den Seiten unterzubringen), aber teuer sind sie nicht - weder in absoluten Zahlen, noch als Anteil am Gesamtbudget für Website-Sicherheit.

An EV SSL-Zertifikaten führt in der Zukunft kein Weg mehr vorbei. Kluge Unternehmen setzen sie bereits ein, und mehr und mehr Kunden wissen um ihre Vorteile und erkennen auf den ersten Blick, wenn eine Website EV SSL verwendet. Dennoch gibt es viele Unternehmen, darunter auch aus Ihrer Branche, die EV SSL noch immer nicht einsetzen und auch keine anderweitigen Maßnahmen ergreifen, um das Vertrauen ihrer Kunden zu stärken. Die Einführung von EV SSL-Zertifikaten und die Umsetzung der oben empfohlenen Maßnahmen sind vor diesem Hintergrund geradezu ein Muss. Wer das Vertrauen seiner Kunden gewinnt, hat einen Wettbewerbsvorteil - mit VeriSign schaffen Sie das.

# 81%

der Online Kunden  
in Großbritannien  
erkennen das VeriSign  
Secured Seal.<sup>6</sup>

<sup>4</sup> Im Dezember 2009 bei zahlreichen Websites aus mehreren Ländern durchgeführte Tests zeigten, dass VeriSign EV SSL-Zertifikate Steigerungen der Abschlussrate zwischen 5 und 87 Prozent, im Durchschnitt über 20 Prozent, bewirken konnten.

<sup>5</sup> Tec-Ed, Januar 2007

<sup>6</sup> 2009 Synovate/GMI study.

## ➤ ÜBER 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 Websites, 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](http://www.verisign.de)**

\*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.

