Symantec | Website Security Solutions

Norton SECURED powered by Symantec

So beeinflusst Vertrauen die Kaufentscheidung von Online-Kunden

Symantec-Bericht

So beeinflusst Vertrauen die Kaufentscheidung von Online-Kunden

Laut Gartner ist „Vertrauen der Dreh- und Angelpunkt für alle Aktivitäten in unserer digitalen Welt“.[1]

Verbraucher müssen Websites und Unternehmen, mit denen sie interagieren, vertrauen können. Sie müssen davon ausgehen können, dass ihre persönlichen Daten geschützt sind und vertraulich behandelt werden.

Vor allem müssen sich Verbraucher darauf verlassen können, dass Unternehmen alle technischen Möglichkeiten ausschöpfen, um sich und ihre Kunden vor Internetkriminellen und deren durchtriebenen Angriffen zu schützen.

Was sagen die Online-Verbraucher?

Vertrauen ist unabdingbar, doch wie gut sind Website-Betreiber darin, bei potenziellen Online-Kunden Vertrauen aufzubauen?

Symantec hat YouGov mit einer Umfrage in Deutschland, Großbritannien, Frankreich und den USA beauftragt. Es sollte festgestellt werden, in welchem Maße Käufer beunruhigt sind und welches Sicherheitsbewusstsein sie an den Tag legen. Man wollte zudem herausfinden, ob Vertrauensmarken einen Einfluss auf die Bereitschaft zum Online-Kauf haben.

Das Ergebnis ist eindeutig: Die Konsumenten sorgen sich um die Sicherheit beim Online-Kauf, doch die meisten wissen, worauf sie achten müssen.

Unternehmen werden oft dazu aufgefordert, SSL-Zertifikate mit Extended Validation zu verwenden, das Ablaufdatum ihres SSL-Zertifikats im Blick zu halten und auf ihren Websites Vertrauensmarken einzusetzen. Doch sprechen Käufer tatsächlich auf diese Maßnahmen an?

Laut unserer Umfrage – ja.

Ein Abschluss kommt mit größerer Wahrscheinlichkeit auf einer Website zustande, der die Kunden vertrauen. Dies hängt u. a. von den oben genannten Vorkehrungen ab.

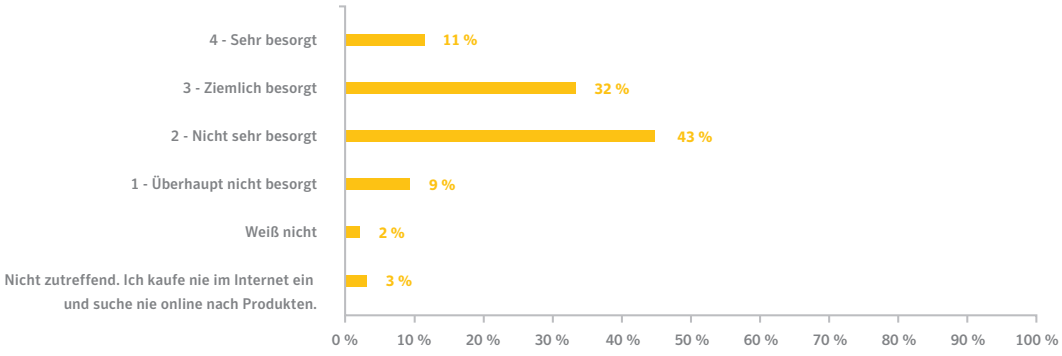
Anders ausgedrückt: Nur wer für ausreichende Website-Sicherheit sorgt, baut Vertrauen bei Kunden auf. Und ohne Vertrauen keine positiven Kaufentscheidungen.

1. NetworkComputing. „Expired Digital Certificates: A Management Challenge“ – http://www.networkcomputing.com/networking/expired-digital-certificates-a-management-challenge/d/d-id/1102269

Alle Angaben stammen von YouGov Plc (sofern nicht anders angegeben). Insgesamt wurden 7541 Volljährige befragt: 2050 in Deutschland, 2102 in Großbritannien, 1011 in Frankreich und 2378 in den USA. Der Umfragezeitraum war vom 3. bis zum 8. September 2015, und die Umfrage wurde online durchgeführt. Die Angaben wurden gewichtet und sind repräsentativ für alle Erwachsenen (ab 18 Jahren) in diesen Ländern.

Wie besorgt sind Ihre Kunden?

F1 Denken Sie an Gelegenheiten, wenn Sie im Internet einkaufen oder nach Produkten suchen. Wie besorgt sind Sie im Allgemeinen in Bezug auf die Sicherheit beim Online-Kauf (z. B. Kreditkartenbetrug, Identitätsdiebstahl)?



Grundlage: Alle online befragten Volljährigen (7541)

Es besteht kein Zweifel: Viele Konsumenten machen sich Sorgen um die Sicherheit beim Online-Kauf. Bei unserer Umfrage waren 43 % der Befragten „sehr“ oder „ziemlich“ besorgt. Nur 9 % gaben an, überhaupt nicht besorgt zu sein.

Website-Betreiber müssen zur Kenntnis nehmen, dass Vertrauen und Sicherheit eine wichtige Rolle bei Verbrauchern spielen. Natürlich sind auch Faktoren wie Preis, Produktqualität und Benutzerfreundlichkeit relevant, aber Sicherheit ist unerlässlich.

Ein Fünftel aller Befragten, die online einkaufen oder nach Produkten suchen, befürchtet insbesondere, dass ihre Zahlungsdaten gestohlen werden. Fast genauso viele Umfrageteilnehmer (19 %) haben in erster Linie Angst vor Identitätsdiebstahl. In den USA beläuft sich diese Zahl sogar auf mehr als ein Drittel (36 %). Diese Bedenken betreffen vor allem die Sicherheit der angegebenen Daten und die Vertrauenswürdigkeit der Personen oder Unternehmen, denen diese Daten anvertraut werden.

Das unterstreicht, wie wichtig vertrauenswürdige (da ist der Begriff schon wieder) SSL- und TLS-Zertifikate sind, die von anerkannten und vertrauenswürdigen Zertifizierungsstellen wie Symantec ausgestellt werden. Diese Zertifikate werden zur Verschlüsselung von persönlichen Angaben und Zahlungsdaten und zur Bestätigung der Identität der Website-Betreiber verwendet. Damit wird den beiden wichtigsten Anliegen der Konsumenten Rechnung getragen.

Warum machen sich Kunden Sorgen?

Es ist kein Wunder, dass Verbraucher sich sorgen: 2014 sah den Verlust oder Diebstahl von 32 Datensätzen[2] pro Sekunde. Bei 80 %[3] der Identitätsdiebstähle (bzw. versuchten Diebstähle) in den ersten drei Monaten in 2015 waren die Täter online zugange.

2. Nasdaq. „Credit card fraud and ID theft statistics“ – http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388#ixzz3mZTlPqsa
3. BBC News. „Number of identity theft victims ‘rises by a third’“ – http://www.bbc.co.uk/news/uk-32890979

Warum sind diese Zahlen so hoch? Weil personenbezogene Daten für Kriminelle von großem Wert sind. Dem aktuellen Symantec-Bericht über Bedrohungen für Websites[4] zufolge erzielen Kreditkartendaten im Internet Schwarzmarktpreise zwischen 0,50 und 20 US-Dollar. Identitätsdaten lassen sich je nach Vollständigkeit für 10 bis 50 US-Dollar verkaufen.

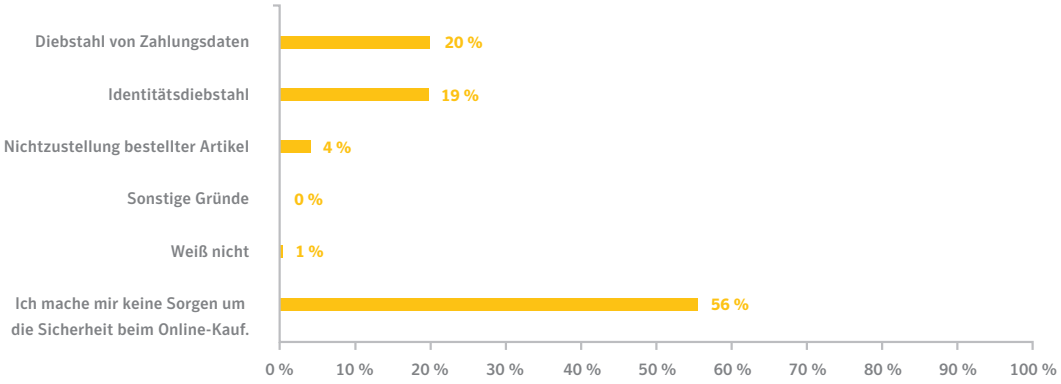
Natürlich sind nicht nur Datenschutzverletzungen und Kartenbetrug Schuld daran, dass Verbraucher Online-Transaktionen misstrauisch gegenüber stehen. Das vermehrte Medieninteresse an Internetkriminalität und hochgradigen Sicherheitsverletzungen schürt ihr Misstrauen zusätzlich.

Bestes Beispiel ist der Angriff auf „Ashley Madison“. Meldungen über Selbstmorde und Promi-Skandale schmückten die ohnehin schon explosive Story über das Fremdgeh-Portal mit reißerischen Einzelheiten aus.

Dazu kommen dann noch Sicherheitsverletzungen bei Regierungsbehörden, wie der Hacker-Angriff auf das amerikanische Office of Personnel Management (OPM) in diesem Jahr[5], bei dem die persönlichen Daten von fast vier Millionen Regierungsangestellten in den USA gestohlen wurden, und die Angst nimmt unweigerlich zu. Wenn das Vertrauen der Bürger in die Netzwerksicherheit der eigenen Regierung derart enttäuscht wird, werden sie wohl kaum ohne weitere Überzeugungsarbeit einer E-Commerce-Website vertrauen.

Mangelnde Besorgnis ist nicht gleich mangelndes Bewusstsein

F2 Sie haben angegeben, dass Ihnen die Sicherheit beim Online-Kauf Sorgen bereitet. Welcher der folgenden Aspekte beunruhigt Sie am meisten bei Kauftransaktionen im Internet? (Bitte wählen Sie die Option aus, die am besten zutrifft.)



Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

Während manche Verbraucher ganz konkrete Bedenken in Bezug auf das Online-Shopping haben, machen sich laut unseren Ergebnissen 56 Prozent der Befragten keine Sorgen über die Sicherheit bei Internetkäufen. Das heißt jedoch nicht, dass diese Kunden keinen Wert auf Sicherheit legen.

Weiter unten in diesem Bericht wird aufgezeigt, dass ein überraschend hoher Anteil der Umfrageteilnehmer nach Zeichen der Seriosität und Vertrauenswürdigkeit Ausschau hält, zum Beispiel nach „https“ und einem Vorhängeschloss in der Adressleiste des Browsers. Diese Antwort so vieler Verbraucher, die nach eigenen Angaben nicht besorgt sind, ist wahrscheinlich darauf zurückzuführen, dass diese Internetnutzer mit den Risiken vertraut sind und sie zu vermeiden wissen.

4. Symantec. „Internet Security Threat Report“, 2015, 20. Ausgabe – http://www.symantec.com/security_response/publications/threatreport.jsp
5. BBC News. „Millions of US government workers hit by data breach“ – http://www.bbc.co.uk/news/world-us-canada-33017310

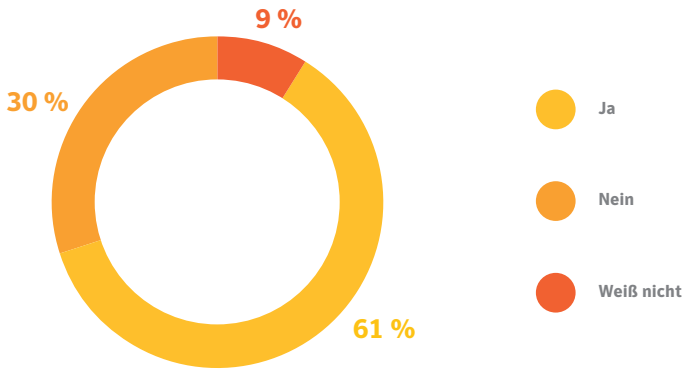
So wichtig ist eine vertrauens-erweckende Adresse

Die richtige Adresse verleiht Ladengeschäften Glaubwürdigkeit. Man denke nur an die Ausstatter in der Savile Row in London, Designer auf der 5th Avenue in New York oder an die Boutiquen auf dem Champs-Élysées in Paris. Wenn Sie ein Geschäft an einer dieser Adressen betreten, wissen Sie, was Sie erwartet.

Dasselbe Prinzip gilt auch im Internet: Das Aussehen Ihrer URL-Adresse kann eine große Rolle bei der Wahrnehmung Ihrer Kunden spielen.

Wir wollten von den Umfrageteilnehmern wissen, ob sie beim Online-Kauf im Allgemeinen auf die Adressleiste des Browsers achten. Das Ergebnis mag Sie überraschen:

Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)



Fast zwei Drittel der Online-Kunden schauen sich beim Shopping die URL in der Adressleiste an, um zu sehen, ob die Website sicher ist. Doch worauf genau wird geachtet?

Die wichtigsten Vertrauenszeichen sind …

- **„https“** (im Gegensatz zum unverschlüsselten „http“) am Beginn der Adresse: Daran erkennen Kunden, dass die Interaktion mit der Website verschlüsselt ist und Internetkriminelle die beim Kauf übermittelten Daten nicht abfangen können.

- **ein graues Vorhängeschloss:** Durch dieses Symbol wird den Verbrauchern signalisiert, dass die Betreiber der Website die Domain gekauft haben. Allerdings wird dadurch nicht die Legitimität des Inhabers bestätigt.

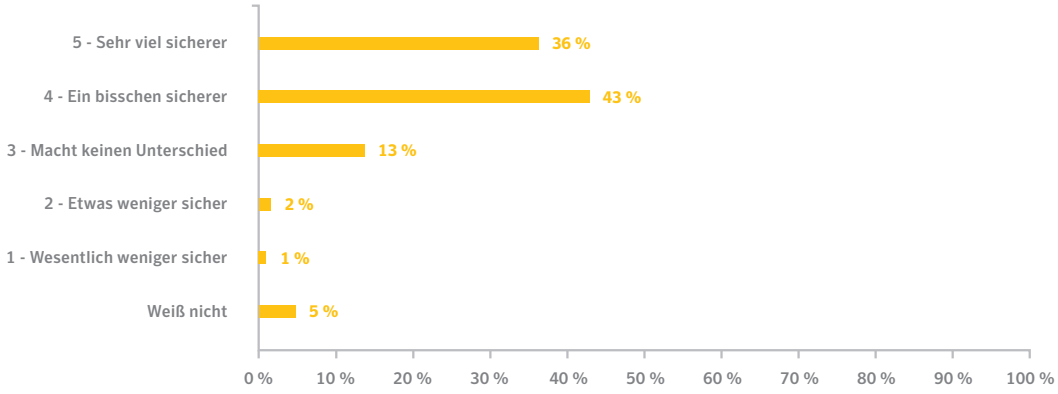
- **ein grünes Vorhängeschloss:** Dies zeigt an, dass die Website SSL mit Extended Validation verwendet. Folglich wurde der Website-Betreiber einer strengen Identitätsprüfung unterzogen, die den Verbrauchern bestätigt, dass es sich bei dem Betreiber auch wirklich um denjenigen handelt, für den er sich ausgibt, und dass dieser Betreiber der Eigentümer der Website ist und die Kontrolle darüber hat.

Wir wissen also, dass Kunden achtgeben. Doch wie reagieren sie?

Wir haben den Teilnehmern die folgende URL-Adresse mit einem Vorhängeschloss gezeigt:

Dann haben wir gefragt, ob sie sich bei einem Online-Kauf sicherer fühlen würden, wenn die URL-Adresse ein Vorhängeschloss enthält (im Vergleich zu einer Adressleiste ohne Schloss).

Beachtliche 78 % (auf zwei Dezimalstellen gerundet) gaben an, dass ein Vorhängeschloss ihnen mehr Sicherheit vermittelt.



Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

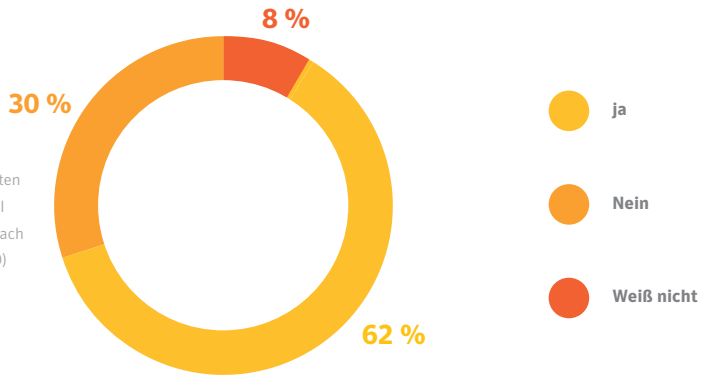
Bei dem gezeigten Beispiel handelte es sich um ein grünes Vorhängeschloss. Dieses Symbol zeigt an, dass die Website SSL mit Extended Validation verwendet, was in den Augen der Verbraucher nicht nur Ihre Website vertrauenswürdig macht, sondern auch Ihr Unternehmen.

Das zeigt einmal mehr: SSL-Zertifikate mit Extended Validation sind unerlässlich für den Aufbau von Vertrauen und Glaubwürdigkeit.

Konversion – eine Frage des Alters?

Laut Nielsen ist „anfängliches Vertrauen die Basis für lebenslange Kundenloyalität“.[6]

Unsere Befragung zeigt auf jeden Fall, dass Vertrauen für alle demografischen Gruppen der Schlüssel zur Konversion ist. Die Frage, ob sie schon einmal einen Kaufvorgang aus mangelndem Vertrauen in die Website abgebrochen hatten, beantworteten die Befragten aller Altersgruppen (und in allen vier Ländern) nahezu gleich.



Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

Wer es nicht schafft, bei seinen Kunden Vertrauen aufzubauen, wird wahrscheinlich keine Konversion erzielen. Doch wie genau Vertrauen gebildet wird, hängt davon ab, worauf Verbraucher der verschiedenen demografischen Kategorien ansprechen.

Junge Konsumenten

Laut einem aktuellen Bericht von Nielsen zum Thema „E-Commerce: Evolution oder Revolution“[6] machen „die Millennials mehr als die Hälfte der Befragten aus (53 Prozent), die Online-Käufe in jeder Produktkategorie dieser Umfrage planen“.

Abgesehen davon, dass die Millennium-Generation den Großteil der Online-Käufer darstellt, lassen die Umfrageergebnisse von Nielsen zum Kaufverhalten in den einzelnen Kategorien auch den Schluss zu, dass „wer einmal online kauft, immer wieder online kaufen wird“.

Früh das Vertrauen der Verbraucher zu gewinnen, kann sich auf Jahre hin auszahlen. Daher müssen Sie wissen, wie Sie junge Konsumenten wirksam erreichen.

6. Nielsen. „E-Commerce: Evolution or revolution in the fast-moving consumer goods world?“ August 2014 – http://ir.nielsen.com/files/doc_financials/Nielsen-Global-E-commerce-Report-August-2014.pdf

Wir haben den Umfrageteilnehmern zwei Abbildungen gezeigt:

Abbildung 1

Abbildung 2

- **Abbildung 1** zeigt, wie eine vertrauenswürdige Website aussehen kann, die SSL mit Extended Validation verwendet (samt grüner Adressleiste und „https“).

- **Abbildung 2** enthält keine Anzeichen der Website-Sicherheit.

SSL mit Extended Validation ist eine wichtige Funktion, doch die Erkennung dieses Merkmals setzt ein gewisses technisches Verständnis voraus. Mehr als zwei Drittel (70 Prozent) der Befragten zwischen 18 und 24 Jahren würden der Website in Abbildung 1 mehr vertrauen und dort eher einkaufen.

Die jüngere Generation kennt sich in Sachen Internetsicherheit besser aus. Junge Konsumenten wissen, worauf sie beim Online-Shopping achten müssen und wem sie vertrauen können. Um diese Kunden zum Kaufen zu bewegen, müssen Sie ihnen die Vertrauenszeichen zeigen, nach denen sie Ausschau halten.

Signalisieren Sie, dass Sie alle möglichen Schritte unternommen haben, um Ihre Seriosität unter Beweis zu stellen und Kundendaten zu schützen. Konkret bedeutet das:

- **SSL mit Extended Validation,** wodurch sich die Adressleiste grün färbt.

- **Vertrauensmarken,** wie das Norton Secured-Siegel, sollten gut sichtbar auf der Website präsentiert werden. Daran erkennen Verbraucher, wer Ihnen vertraut.

- **Always-On SSL stellt sicher,** dass jede Interaktion mit Ihrer Website (ob Surfing oder Kauf) verschlüsselt wird.

Nicht mehr ganz so junge Konsumenten

Euromonitor[7] schätzt, dass 2020 die Kaufkraft der Verbraucher ab 60 Jahren weltweit 15 Billionen US-Dollar betragen wird. Und der Stereotyp von den Großeltern, die nicht mal den Computer anschalten können, ist mittlerweile völlig passe.

Laut Business Insider Intelligence „kauft ein überproportional hoher Anteil von Verbrauchern mittleren Alters im Internet ein". Und in den USA ist einer von vier Online-Kunden älter als 55. „Mit der zunehmenden Alterung der Bevölkerung werden prozentual immer mehr Verbraucher online gehen, und die Anzahl der Internetbenutzer wird weiterhin steigen", bestätigt John Burbank, President Strategic Initiatives bei Nielsen.

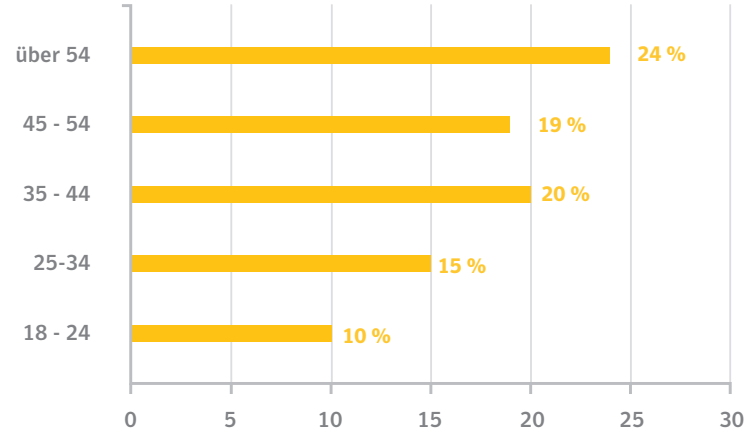
Die ältere Generation wächst schnell, ist finanziell gut situiert und technisch immer versierter. Allerdings braucht diese Bevölkerungsgruppe mehr Rückversicherung als jüngere Käufer und nicht ganz so technische Sicherheitshinweise.

Besorgte Konsumenten

Kommen wir wieder zurück zu unserer Umfrage. Fast die Hälfte der Befragten (48 Prozent) ab 55 Jahren macht sich Sorgen um die Sicherheit beim Online-Shopping. Das steht im Gegensatz zu nur 34 Prozent der 18- bis 24-Jährigen.

Und wenn es um die konkreten Bedenken bei Internetkäufen geht, sorgen sich die Verbraucher mit zunehmendem Alter generell mehr um Identitätsdiebstahl.

So viele Befragte (in Prozent), die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben, sorgen sich beim Online-Shopping am meisten um „Identitätsdiebstahl".



Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

Unsere Ergebnisse zeigen, dass ältere Verbraucher technisch weniger versiert sind. Bei denselben beiden Abbildungen von Websites, die auch 18- bis 24-Jährigen gezeigt wurden (eine mit SSL mit Extended Validation und eine ohne sichtbare Sicherheitsmerkmale) wählten nur 29 Prozent der Altersgruppe ab 55 die Website, die SSL mit Extended Validation verwendet, als vertrauenswürdigere Option beim Online-Shopping aus.

7. Financial Times. „The Silver Economy: Baby boomers power new age of spending." 7. Nov. 2014 – http://www.ft.com/cms/s/0/e9fc95c0-44b1-11e4-ab0c-00144feabdc0.html#axzz3mZB73kbn

Für diese Gruppe von Käufern müssen Sie Ihre Glaubwürdigkeit auf einfachere Weise demonstrieren. Laut unserer Umfrage sind Vertrauensmarken die beste Lösung.

Wir haben folgende Frage gestellt:
Stellen Sie sich vor, Sie surfen im Internet und sind kurz davor, einen Kauf abzuschließen. Welcher der abgebildeten Websites würden Sie eher vertrauen?

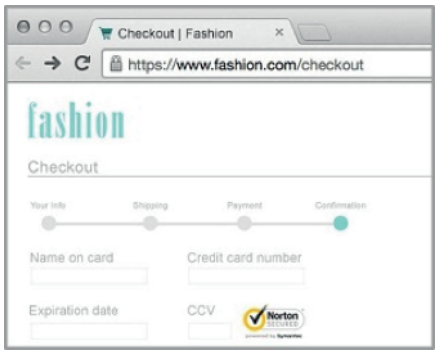
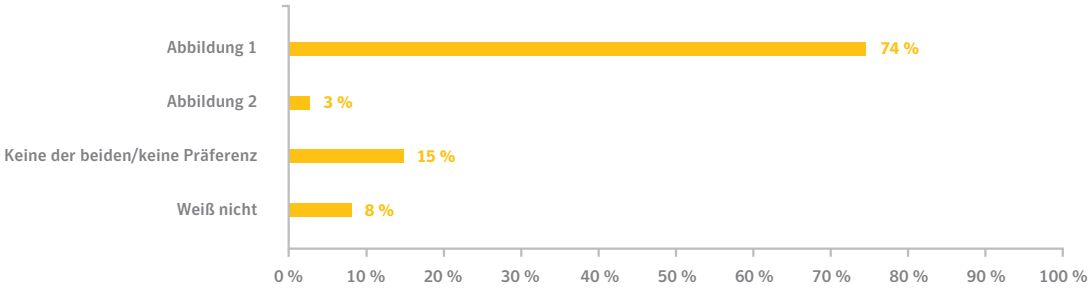


Abbildung 1

Abbildung 2

Fast drei Viertel (74 Prozent) wählten Abbildung 1, die Website mit dem Norton Secured-Siegel. Diese deutliche Präferenz war bei allen Altersgruppen konsistent.



Base: All adults online who ever shop/browse for items online (7330)

Um also alle Altersgruppen anzusprechen, sollten Sie sowohl SSL mit Extended Validation als auch Vertrauensmarken verwenden.

Die Vertrauensmarke als Unterscheidungsmerkmal

Wie wir gesehen haben, kann das Norton Secured-Siegel unabhängig von der Zielgruppe erheblichen Einfluss darauf haben, ob ein Kunde Ihrer Website beim Kaufabschluss mehr Vertrauen schenkt.

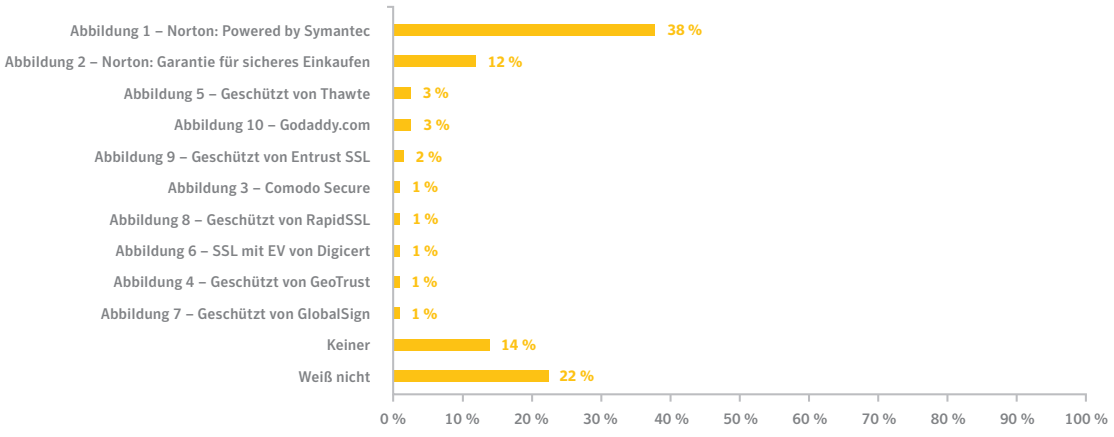
Vertrauensmarken können an jeder beliebigen Stelle auf Ihrer Website platziert werden. Allerdings zeigen Studien, dass sie neben den kritischsten bzw. sensibelsten Feldern in einem Formular am wirkungsvollsten sind. Bei einem Experiment[8] wurde durch das Verschieben der Vertrauensmarke vom oberen Seitenrand hin zum Formular die Konversionsrate um sechs Prozent erhöht.

Welche Rolle spielt der Name?

Nicht nur die Position der Vertrauensmarke wirkt sich auf die Wahrnehmung bei potenziellen Kunden aus, sondern auch der Name der Vertrauensmarke.

An einer Vertrauensmarke erkennt der Besucher einer Website im Prinzip, dass eine unabhängige Stelle diese Website geprüft und für vertrauenswürdig befunden hat. Damit wird suggeriert, dass der Besucher ihr auch vertrauen kann. Die Meinung einer anerkannten, glaubwürdigen Partei hat dabei natürlich mehr Gewicht als ein völlig unbekannter Name.

Wir haben gefragt, welcher der folgenden Vertrauensmarken unsere Teilnehmer beim Online-Shopping am meisten vertrauen würden. Die Vertrauensmarken wurden in keiner bestimmten Reihenfolge präsentiert.



Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

8. Conversion Voodoo. „Proper placement of you 'trust logos' will improve conversion rates" – http://www.conversionvoodoo.com/blog/2012/05/proper-placement-of-your-trust-logos-will-improve-your-conversion-rate/

Symantecs Glaubwürdigkeit spricht für sich selbst: Beinahe die Hälfte der Befragten (49 Prozent) entschieden sich für eine der beiden Vertrauensmarken von Symantec: das Norton Secured-Siegel bzw. die Garantie für sicheres Einkaufen.

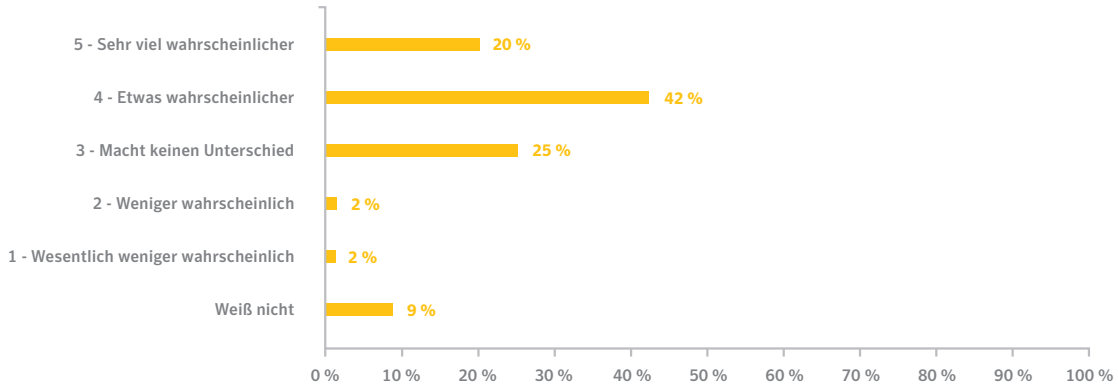
Wie unser Bericht zeigt, ist Vertrauen ein immens wichtiger Faktor für Konversionsraten. Doch Vertrauen alleine führt nicht automatisch zu einem Kauf. Wir wollten daher mehr über den Zusammenhang zwischen einer Symantec-Vertrauensmarke und einem Kaufabschluss herausfinden.

Dazu haben wir den Umfrageteilnehmern das Norton Secured-Siegel präsentiert, das täglich mehr als 500 Millionen Mal auf Websites in 170 Ländern angezeigt wird.

Norton™ SECURED
powered by Symantec

Wir haben gefragt, ob die Verbraucher mit größerer Wahrscheinlichkeit eine Transaktion oder einen Kauf im Internet abschließen würden, wenn dieses Symbol auf der Zahlungsseite einer Website angezeigt wird.

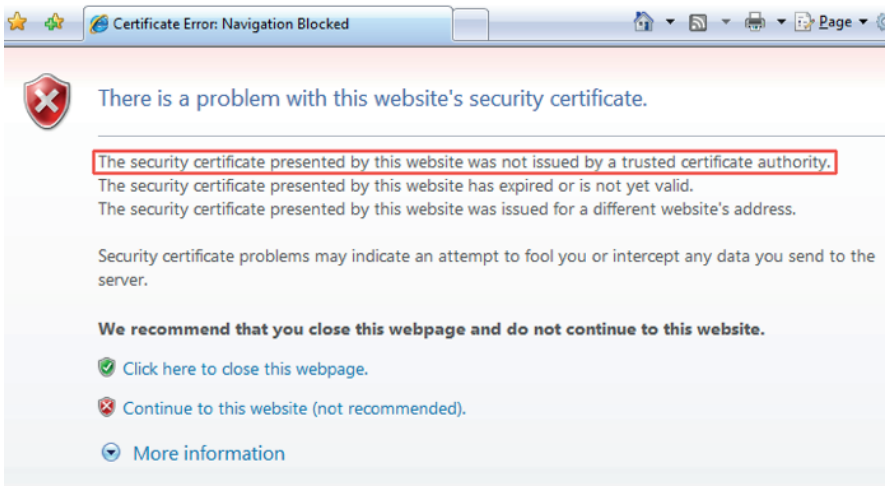
Fast zwei Drittel (63 % auf zwei Dezimalstellen gerundet) bejahten dies.



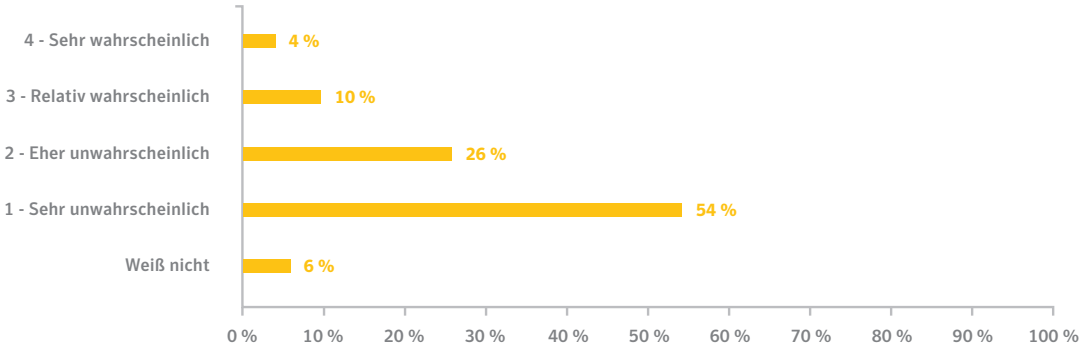
Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

Was passiert bei Problemen? Wie reagieren Verbraucher auf Sicherheitswarnungen?

Vertrauen bei Online-Verbrauchern aufzubauen ist wichtig, doch Sie müssen ebenso intensiv daran arbeiten, dieses Vertrauen zu bewahren. Wenn Sie versäumen, ein abgelaufenes SSL-Zertifikat zu erneuern, wird den Besuchern Ihrer Website eine Sicherheitswarnung angezeigt. Die folgende Abbildung wurde den Umfrageteilnehmern präsentiert:



Wir fragten, mit welcher Wahrscheinlichkeit sie den Besuch einer Website fortsetzen würden, wenn diese Warnung angezeigt wird. Die Antworten zeigen, dass die meisten Online-Kunden eine derartige Warnung als Vertrauensbruch empfinden. 80 Prozent der Befragten halten es für eher oder sehr unwahrscheinlich, dass sie die Website wie ursprünglich geplant aufrufen.



Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

Ähnlich wie bei anderen Ergebnissen in unserer Umfrage schreckt eine solche Warnung Verbraucher mit zunehmendem Alter mehr ab. Zwei Drittel der Online-Shopper ab 55 gaben an, dass ein Besuch der Website sehr unwahrscheinlich sei. Nur 41 Prozent der 18- bis 24-Jährigen entschieden sich für diese Option.

Welche negative Wirkung Sicherheitswarnungen auf die Glaubwürdigkeit einer Website haben, sollte nicht überraschen. Zum einen ist genau das der Grund für Sicherheitswarnungen (Besucher davor zu warnen, dass die entsprechende Website nicht bedingungslos vertrauenswürdig ist), und zum anderen bestätigt eine Umfrage der University of California in Berkeley[9], dass die meisten Verbraucher Sicherheitswarnungen ernst nehmen:

Im Rahmen unserer Feldstudie haben Benutzer ein Zehntel der Malware- und Phishing-Warnungen in Mozilla Firefox, ein Viertel der Malware- und Phishing-Warnungen in Google Chrome und ein Drittel der SSL-Warnungen in Mozilla Firefox ignoriert. Dies zeigt, dass Sicherheitswarnungen in der Praxis funktionieren.

Als Website-Betreiber oder Manager mit Verantwortung für die Website-Sicherheit müssen Sie daher Ihre SSL-Verwaltung optimieren und sicherstellen, dass Sie die SSL-Sicherheit in Ihrem Unternehmen im Griff haben. Frühzeitige Warnungen vor Ablauffristen können den Unterschied zwischen einem neuen Kunden und mehreren abgeschreckten Interessenten bedeuten.

Das Zitat aus der Studie der UC Berkeley belegt außerdem, dass Sie Ihre Website regelmäßig auf Schwachstellen und Malware überprüfen müssen. Malware-Warnungen schrecken potenzielle Kunden ebenfalls oftmals von einem Besuch Ihrer Website ab. Auch Suchmaschinen überprüfen Websites auf Malware und blockieren infizierte Websites. Dies kann verheerende Auswirkungen auf die Anzahl der Internetnutzer haben, die Ihre Website aufrufen.

9. Usernix. „Alice in Warningland: A large scale field study of browser security warning effectiveness“ – https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe

Regionale Unterschiede

Dieser Bericht befasst sich im Großen und Ganzen mit den gesammelten Ergebnissen, die YouGov aus Großbritannien, Deutschland, Frankreich und den USA zusammengetragen hat. Einige regionale Unterschiede innerhalb Europas sind jedoch erwähnenswert.

Großbritannien: eine Insel sicherheitsaffiner Verbraucher

„Gute Online-Sicherheit bildet die Grundlage der gesamten digitalen Wirtschaft. Sie schützt unsere Unternehmen, Bürger und öffentlichen Dienste … Das Vertrauen in die britische Online-Sicherheit ist für Verbraucher, Betriebe und Investoren unerlässlich."

So äußert sich der britische Minister für digitale Ökonomie[10], Ed Vaizey. Die Ergebnisse unserer Umfrage bestätigen die starke Ausrichtung Großbritanniens auf Verbrauchersicherheit und -aufklärung.

Bei der Frage nach ihrer Sorge um die Sicherheit beim Online-Shopping machten die britischen Befragten mit nur vier Prozent den niedrigsten Anteil der Teilnehmer aus, die mit „sehr besorgt" antworteten. Beinahe zwei Drittel (63 Prozent) sind „nicht sehr" oder „überhaupt nicht" besorgt. Diese Zahl liegt deutlich höher als die Gesamtzahl von 52 Prozent.

Das mag daran liegen, dass britische Verbraucher aufgrund von Informationskampagnen wie „Get Safe Online" gut darüber informiert sind, woran sie eine sichere Website erkennen können. Großbritannien verzeichnete den niedrigsten Prozentsatz der befragten Online-Shopper, die eine Website trotz einer Sicherheitswarnung besuchen würden (nur 11 % gaben „sehr" oder „relativ wahrscheinlich" an).

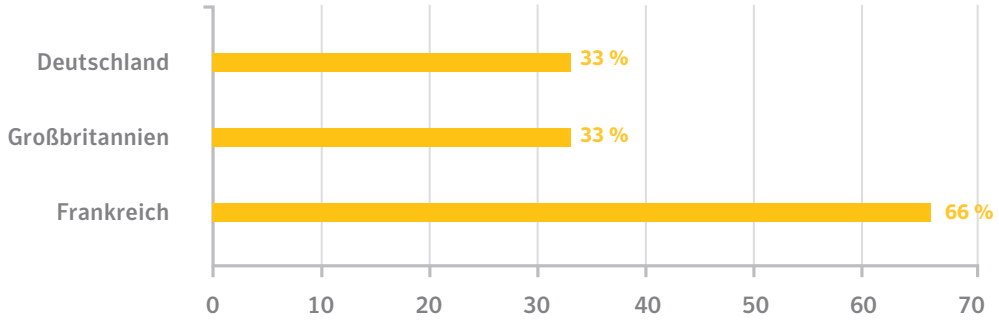
Und als Reaktion auf die Abbildung einer URL-Adressleiste mit Vorhängeschloss gaben 43 Prozent an, dass sie sich durch dieses Symbol „sehr viel sicherer" beim Online-Kauf fühlen würden. Diese Zahl ist wesentlich höher als die durchschnittliche globale Gesamtzahl (36 Prozent).

10. ComputerWeekly.com. „Majority of UK business have been targeted by cyber criminals." – http://www.computerweekly.com/news/4500253942/Majority-of-UK-businesses-have-been-targeted-by-cyber-criminals

Frankreich: ein Land unsicherer Verbraucher

Die französischen Umfrageteilnehmer machten sich wesentlich größere Sorgen um die Sicherheit beim Online-Shopping als jede andere Nation. Zwei Drittel sind „relativ“ oder „sehr besorgt“ (im Gegensatz zur Gesamtzahl von nur 43 Prozent).

Prozentsatz der Befragten, die „sehr“ oder „relativ“ besorgt um die Sicherheit beim Online-Shopping sind



Grundlage: Alle online befragten Volljährigen, die schon einmal im Internet eingekauft oder nach Artikeln gesucht haben (7330)

Die Hälfte der französischen Befragten, die online einkaufen, sorgt sich hauptsächlich um den Diebstahl von Zahlungsdaten (Gesamtzahl: ein Fünftel).

Doch ungeachtet ihrer Bedenken würden die Verbraucher in Frankreich trotz einer Sicherheitswarnung eher den Besuch einer Website fortsetzen. Mehr als ein Viertel (26 Prozent) würde die Website „sehr“ oder „relativ“ wahrscheinlich aufrufen (Gesamtzahl: 14 Prozent).

Wenn französische Internetnutzer Websites mit abgelaufenen oder widerrufenen SSL-Zertifikaten besuchen, haben sie auch allen Grund zur Sorge.

Deutschland: alles andere als leichtgläubig

Laut unseren Umfrageergebnissen lassen sich deutsche Verbraucher nicht so schnell von Vertrauenszeichen überzeugen.

In Reaktion auf eine URL-Adressleiste mit grünem Vorhängeschloss fühlt sich beispielsweise nur ein Viertel der Online-Shopper in Deutschland „sehr viel sicherer" – im Gegensatz zu 43 Prozent in Großbritannien und Frankreich.

Wir zeigten den Befragten zwei Abbildungen: eine Website mit „https", einem Vorhängeschloss und dem Norton Secured-Siegel und eine Website ganz ohne Vertrauenshinweise. Nur zwei Drittel der Deutschen gaben die erste Website als mehr vertrauenswürdig an. 21 Prozent erklärten, dass sie keiner der beiden Kaufoptionen mehr vertrauen würden. Die Gesamtzahlen lagen jeweils bei 74 und 15 Prozent.

Eine vom Deutschen Institut für Vertrauen und Sicherheit im Internet[11] veröffentlichte Studie bestätigt, dass sich das Online-Sicherheitsgefühl der Deutschen deutlich verschlechtert hat. Dies mag erklären, warum bestimmte Sicherheitsmerkmale in unserer Umfrage auf eine weniger positive Resonanz gestoßen sind.

Anderseits ist da der 2014[12] veröffentlichte Bericht zur IT-Sicherheitslage vom Deutschen Bundesamt für Sicherheit in der Informationstechnik:

„Trotz erhöhter Sensibilisierung [in Bezug auf Sicherheitslücken] und schlechterem Sicherheitsgefühl [gegenüber dem Internet] werden konkrete Schutzmaßnahmen in der Praxis nur geringfügig häufiger umgesetzt."

Es ist natürlich möglich, dass deutsche Verbraucher sich nicht kundig gemacht haben und daher nicht wissen, worauf sie beim Online-Shopping achten müssen.

Website-Betreiber in Deutschland müssen ernsthafte Anstrengungen unternehmen, um das Vertrauen potenzieller Kunden zu gewinnen. Aufgrund einer kürzlich erfolgten Gesetzesänderung[13] können Website-Betreiber in Deutschland mit einem Bußgeld belegt werden, wenn sie ihre Website-Sicherheit nicht auf dem neuesten Stand halten. Dies mag zur Entschärfung des Problems beitragen, aber letztendlich besteht die Forderung der Konsumenten nach Glaubwürdigkeit und Sicherheit.

11. DDIVSI. „PRISM und die Folgen: Sicherheitsgefühl im Internet verschlechtert", 3. Juli 2013 – https://www.divsi.de/prism-und-die-folgen-sicherheitsgefuehl-im-internet-verschlechtert/

12. FBundesamt für Sicherheit in der Informationstechnik. „Die Lage der IT-Sicherheit in Deutschland 2014" – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

13. FFriedrich Graf von Westphalen & Partner. „Bundestag verabschiedet IT-Sicherheitsgesetz" – http://www.fgvw.de/2704-0-Bundestag+verabschiedet+IT-Sicherheitsgesetz.html

So bauen Sie zusammen mit Symantec Kundenvertrauen auf

Symantec ist ein führender Anbieter im Bereich der Website-Sicherheit und schützt mehr als eine Million Webserver und 91 Prozent der Fortune-500-Unternehmen weltweit.

Wir bieten eine breite Palette an Produkten und Services, mit denen Sie Vertrauen bei Ihren Kunden schaffen und Ihre Konversionsraten verbessern können.

Produkt	Details	Unterstützung beim Vertrauensaufbau
Symantec SSL- und TLS-Zertifikate	Wir bieten eine Auswahl an SSL-Zertifikaten zum Schutz externer und interner Websites.	SSL-Zertifikate belegen die Legitimität des Website-Betreibers und gewährleisten einen verschlüsselten Datenaustausch zwischen Besucher und Website. So wird verhindert, dass Internetkriminelle vertrauliche Daten während der Übertragung abfangen.
SSL mit Extended Validation	Wir unterziehen Unternehmen einer strikten Identitätsprüfung. So belegen wir die Legitimität Ihres Unternehmens und stellen sicher, dass Ihr Unternehmen bei den entsprechenden Stellen registriert ist.	Beim Aufruf einer Website, die SSL mit Extended Validation verwendet, wird die Adressleiste grün gefärbt bzw. ein grünes Vorhängeschloss angezeigt. Damit belegen Sie Ihren Kunden gegenüber die Legitimität Ihres Unternehmens und Ihrer Website.
Das Norton Secured-Siegel	Wie der Bericht zeigt, können Sie diese Vertrauensmarke verwenden, wenn Sie Ihre Website mit einem SSL-Zertifikat von Symantec schützen.	Daran erkennen Website-Besucher, dass Ihre Website das Vertrauen einer anerkannten Partei genießt. Laut unseren Umfrageergebnissen sprechen Kunden gut auf dieses Siegel an, und frühere Studien belegen, dass es sich um die bekannteste Vertrauensmarke im Internet handelt.
Seal-in-Search	Für Internetnutzer, die ein Sicherheits-Plug-in in ihrem Browser aktiviert haben, wird in den Ergebnislisten von Suchmaschinen, auf Partnerwebsites und auf Produktbewertungsseiten das Norton Secured-Siegel neben dem Link zu Ihrer Website angezeigt.	So können Sie schon vor einem Besuch Ihrer Website Vertrauen bei Kunden aufbauen, damit diese sich für Ihre Website und nicht für ein anderes Angebot in den Suchergebnissen entscheiden.

Produkt	Details	Unterstützung beim Vertrauensaufbau
Norton-Garantie für sicheres Einkaufen	Diese Option enthält drei 30-Tage-Garantien für Ihre Kunden: • Schutz gegen Identitätsdiebstahl (bis zu 10.000 US-Dollar) • Bürgschaft eines Dritten für Ihre Verkaufsbestimmungen (bis zu 1.000 US-Dollar) • Tiefstpreisgarantie bis zu 100 US-Dollar	Damit geben Sie Ihren Kunden zu erkennen, dass Sie Vertrauen in Ihre Website haben und dass sich für Ihre Kunden im Fall der Fälle keine Nachteile ergeben.
Schwachstellenanalysen und Malware-Scans	Zusammen mit bestimmten SSL-Zertifikaten von Symantec erhalten Sie automatische wöchentliche Schwachstellenanalysen und tägliche Malware-Scans gratis.	2014 fanden sich bei drei Viertel der geprüften Websites[4] Schwachstellen – ein Fünftel davon waren äußerst bedenklich. Wenn Sie Malware nicht umgehend entfernen, gefährden Sie auch Ihre Kunden. Außerdem erhöht sich die Wahrscheinlichkeit, dass Ihre Website eine Sicherheitswarnung auslöst. Mit regelmäßigen Scans können Sie dies vermeiden.
Erkennung und Automatisierung	Mit den Tools zur Erkennung und Automatisierung von Symantec können Sie Ihre SSL-Infrastruktur verwalten und sicherstellen, dass alle Zertifikate von einer anerkannten Zertifizierungsstelle ausgestellt wurden. Darüber hinaus werden Sie frühzeitig über Ablauffristen der SSL-Zertifikate benachrichtigt.	Wie wir gesehen haben, erodieren abgelaufene SSL-Zertifikate das Vertrauen Ihrer Kunden. Je größer ein Unternehmen wird, desto schwieriger ist es, sämtliche SSL-Zertifikate im Blick zu behalten. Und desto eher wird ein Erneuerungsdatum übersehen. Mit den Tools von Symantec lässt sich dies vermeiden.

Wenn Sie mehr darüber erfahren möchten, wie Sie zusammen mit einem weltweit anerkannten Partner für Internetsicherheit Vertrauen schaffen, nehmen Sie noch heute mit Symantec Kontakt auf.

4. Symantec. „Internet Security Threat Report“, 2015, 20. Ausgabe – http://www.symantec.com/security_response/publications/threatreport.jsp

Symantec | Website Security Solutions

Norton SECURED powered by Symantec

Über Symantec

Symantec ist ein weltweit führender Anbieter von Lösungen in den Bereichen Informationssicherheit, Datenspeicherung und Systemmanagement, die Privatkunden und Unternehmen bei der Sicherung und Verwaltung ihrer datengesteuerten Welt unterstützen. Unsere Software und Services vermitteln Vertrauen, unabhängig davon, wo Daten verwendet werden oder gespeichert sind.