

## Executive Summary

CONSUMER MARKETS

### **Executive Summary zur KPMG-Studie „Sicherheitsempfinden im Onlinehandel“**



# Sicherheitsempfinden im Onlinehandel

Das Internet ist im Alltag selbstverständlich geworden. Es dient der Kommunikation, dem Meinungs austausch, der Darstellung der eigenen Person und ersetzt zunehmend auch traditionelle Einkaufskanäle.

Unsere aktuelle Studie „Sicherheitsempfinden im Onlinehandel“ zeigt, dass Sicherheitsbedenken sowohl im Onlinehandel als auch bei der Nutzung sozialer Netzwerke eine ausgeprägte Rolle spielen. Der Onlinehandel hat dies bereits erkannt und versucht, mit gezielten Maßnahmen das Vertrauen der Kunden in den Onlinekauf zu stärken.

Die Sicherheitsbedenken der Nutzer in Bezug auf die Datenspeicherung in sozialen Netzwerken sind mit Blick auf die zunehmende Verbindung des klassischen Onlinehandels mit Funktionen

sozialer Netzwerke durchaus kritisch zu interpretieren. Während es dem klassischen Onlinehandel gelingt, das Vertrauen in digitales Einkaufen stetig zu erhöhen, wird die Nutzung sozialer Medien zur Steigerung des Absatzes nur dann erfolgreich sein, wenn das Sicherheitsempfinden auf ein vergleichbares Niveau angehoben wird.

Unser Executive Summary zeigt anhand von sechs Kernthemen Ansatzpunkte zur Optimierung des Onlineauftritts, die das Kundenvertrauen verbessern, die Reputation des Unternehmens absichern und so den Absatz über Onlinekanäle fördern können.

Wir wünschen Ihnen eine anregende Lektüre und freuen uns, die Ergebnisse der Untersuchung und unsere Handlungsansätze persönlich mit Ihnen zu diskutieren.

Die detaillierten Ergebnisse entnehmen Sie bitte der Gesamtstudie.

Gern stellen wir Ihnen diese unter [www.kpmg.de/sicherheitsempfinden](http://www.kpmg.de/sicherheitsempfinden) zur Verfügung.



**Wolfgang Geesmann**  
Partner,  
Information Risk Management



**Lars Hartke**  
Senior Manager,  
Information Risk Management

## Hintergrund und Umfang der Studie

Die Studie „Sicherheitsempfinden im Onlinehandel“ untersucht das Konsumentenverhalten hinsichtlich der Preisgabe persönlicher Daten und wie sich die Sicherheitsbedenken beim Onlinekauf von denen bei der Nutzung sozialer Netzwerke unterscheiden. Zudem evaluiert sie, welche vertrauensbildenden Maßnahmen getroffen werden können und ob Kunden bereit sind, für solche Maßnahmen zu zahlen. Konkret wird die Wirkung von Gütesiegeln, ausgewählten Zahlungsverfahren und Kundenbewertungen analysiert.

In Zusammenarbeit mit dem E-Commerce-Center Handel (ECC Handel) hat KPMG eine Onlinebefragung mit 1.019 Teilnehmern ab 16 Jahren in Deutschland (repräsentative Stichprobe der Internetpopulation) durchgeführt.

# Studienergebnisse zu vertrauensbildenden Maßnahmen und Sicherheitsaspekten im Onlinehandel

## ■ Nutzungsbarrieren identifizieren, Positivattribute nutzen

Die größte Nutzungsbarriere im E-Commerce sind Bedenken, dass persönliche Daten von Onlineshopbetreibern für Werbezwecke an Dritte weitergegeben und vertrauliche Daten beziehungsweise Zahlungsinformationen ausspioniert oder missbraucht werden. Onlinehändler sollten daher verstärkt die positive Wirkung von Gütesiegeln und Kundenbewertungen als vertrauensbildende Maßnahmen nutzen. Durch entsprechende Marketingmaßnahmen, neutrale Gutachten und Einholung positiver Kundenrückmeldungen können sich Anbieter entsprechend im Markt positionieren.

## ■ Transparente Bezahlwege schaffen, Kaufabbrüche reduzieren

Die Ergebnisse zeigen, dass Unternehmen gut beraten sind, die Sicherheitsbedenken, die mit der Angabe von Kreditkarten- oder Bankverbindungsdaten zusammenhängen, ernst zu nehmen. Das fehlende Angebot von anderen Zahlungsarten als Vorkasse ist der häufigste Grund für Kaufabbrüche.

Unternehmen sollten den Nutzern eine Auswahl verschiedener Zahlungsverfahren anbieten, insbesondere Rechnungszahlung oder internetspezifische Bezahldienste. Da die Befragten eine deutliche Bereitschaft zeigen, für ein sicheres und transparentes Zahlverfahren einen höheren Preis zu zahlen, können Onlinehändler ein entsprechendes Angebot beziehungsweise die Bereitstellung von Zahlungsalternativen auch in ihrer Preisgestaltung berücksichtigen.

## ■ Persönliche Datenangaben im Kaufprozess begrenzen

Die Angabe sensibler Daten im Rahmen des Kauf- beziehungsweise Bestellprozesses gehört zu den häufigsten Gründen, warum einige Internetnutzer nach wie vor nicht online einkaufen. Die Angaben auf den Onlineformularen sollten deshalb auf die für den Kauf- beziehungsweise Bestellprozess unbedingt erforderlichen Daten beschränkt werden.

## ■ Datensicherheit und Datenschutz zur „Chefsache“ machen

Das Management von Online- und Multi-Channel-Anbietern muss sich deutlich für Datensicherheit und Datenschutz aussprechen und diese Selbstverpflichtung auch im Onlineauftritt verdeutlichen. Das Vertrauen von Onlinenutzern hängt stark mit der Reputation des Anbieters zusammen. Datensicherheit ist unternehmensintern sowie nach außen zu organisieren und kontrollieren.

Auf Verkäuferseite sind erhöhte Sicherheitsvorkehrungen in Bezug auf kauf- und zahlungsbezogene Kundendaten vorzunehmen, bis hin zu der Frage, inwieweit eingebundene Bezahldienste als Serviceprovider Kundendaten nutzen dürfen.

## ■ Den Nutzen sozialer Medien als Absatzkanal verdeutlichen

Der Nutzen sozialer Netzwerke im Rahmen des Onlineshoppings ist zahlreichen Kunden noch nicht klar. Da aber immer mehr Menschen in sozialen Netzwerken aktiv sind und soziale Netzwerke auch zunehmend im beruflichen Umfeld genutzt werden, sollten ihre Betreiber sich ernsthaft mit den Sicherheitsbedenken der Internetnutzer auseinandersetzen und Maßnahmen ergreifen, um die subjektiv wahrgenommene Sicherheit zu erhöhen.

Um den Sicherheitsbedenken der Nutzer zu begegnen, müssen die Betreiber sozialer Netzwerke ihren Umgang mit privaten Daten, Datenschutz, Datenlöschung etc. deutlich transparenter gestalten und für wirksame Kontrollmechanismen sorgen.

## ■ IT-Sicherheits- und Reputationsrisiken identifizieren

Der wachsende Trend zur Nutzung von Onlineshops mit internetspezifischen beziehungsweise mobilen Bezahl-systemen ist verbunden mit neuen Risiken in Bezug auf Datenschutz und IT-Sicherheit, insbesondere die Unternehmensreputation.

Neben der sicheren und komfortablen Bezahlfunktion sind für den Verbraucher der Datenschutz und das Wissen, welche Daten wie und an welcher Stelle weiterverwendet werden, von hoher Bedeutung. Entscheidend ist, dass diese Transaktionen nicht korrumpierbar sind. Unternehmen sollten frühzeitig ihre individuelle Risikosituation durch eine neutrale Instanz bewerten lassen, um zielgerichtet Sicherheits- und Kontrollmaßnahmen aufzusetzen. Risikomanagement in Bezug auf Informationssicherheit wird durch Standards wie ISO 27001 abgedeckt.

# Bestens für Sie aufgestellt

Durch eine Jahrzehnte währende Prüfungs- und Beratungspraxis verfügt KPMG über eine umfassende nationale und internationale Branchenexpertise im Handel und in der Konsumgüterindustrie. Unsere Lösungsansätze sind eindeutig, ganzheitlich und praxisnah und tragen unterschiedlichsten Geschäftsmodellen und Unternehmensgrößen Rechnung. Durch unsere interdisziplinäre Arbeitsweise verbinden wir unseren tief greifenden Erfahrungsschatz mit dem weitverzweigten Spezialisten-Know-how aus anderen KPMG-Mitgliedsfirmen. Im Sektor

Consumer Markets sind weltweit etwa 2.000 Partner und Manager sowie rund 5.000 fachliche Mitarbeiter tätig. In Deutschland betreut KPMG zurzeit aktiv mehr als 1.000 Mandate in diesem Bereich.

Unser Data Security Team unterstützt Sie dabei, sichere und effiziente Bestell- und Bezahlstrukturen aufzubauen, die gleichzeitig den rechtlichen Anforderungen genügen. Dabei werden Datenströme der Bezahltransaktionen transparent gemacht, Kontrollen systematisch in ein internes Kontrollsystem eingebunden und Risikokosten gesenkt.

Die Informationssicherheit, auch im Hinblick auf an Serviceprovider ausgelagerte Prozesse, kann nach internationalen Standards von unseren Spezialisten geprüft oder zertifiziert werden.

Gern unterstützen wir auch Ihr Unternehmen. Sprechen Sie mit uns!

---

## Kontakt

KPMG AG  
Wirtschaftsprüfungsgesellschaft

### Mark Sievers

Head of Consumer Markets  
T +49 40 32015-5840  
marksievers@kpmg.com

### Wolfgang Geesmann

Partner,  
Information Risk Management  
T +49 211 475-7131  
wgeesmann@kpmg.com

### Lars Hartke

Senior Manager,  
Information Risk Management  
T +49 221 2073-1470  
lhartke@kpmg.com

[www.kpmg.de](http://www.kpmg.de)

## Aktuelle Studien des Sektors Consumer Markets



Trends im Handel  
2020



Preisportale,  
Couponing, soziale  
Netzwerke – der  
Einfluss aktueller  
Online-Trends auf  
das Kaufverhalten

[www.kpmg.de/consumermarkets](http://www.kpmg.de/consumermarkets)

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Konzerngesellschaft der KPMG Europe LLP und Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und „cutting through complexity“ sind eingetragene Markenzeichen von KPMG International.