eKomi
The Feedback Company

Trustsignale für Online-Shops

Einleitung

Die Verwendung von Trustsignalen, darüber sind sich E-Commerce-Experten einig, sind aus einem modernen Onlineshop nicht mehr wegzudenken. Etliche Studien belegen die positiven Effekte, die vertrauensschaffende Maßnahmen auf den Kaufentscheidungsprozess von Online-Shoppern haben.

Eine Studie des ECC-Handel belegte sogar, dass der gezielte Einsatz von Trustsignalen die Conversion-Rate im Schnitt um 23,4 % erhöht. Eine anschließende Online-Umfrage ergab sogar, dass 74 % der User auf Gütesiegel wie eKomi bei der Auswahl eines Online-Shops achten. 64 % gaben an, dass sie einen geprüften Onlineshop gegenüber einem Shop ohne Gütesiegel vorziehen. Der Einsatz von Kundenbewertungen führt sogar zu einer Steigerung der Conversion-Rate um 25 %.

Gütesiegel sorgen dafür, dass der User sich sicher fühlt und reduzieren Kaufabbrüche. Mittlerweile ist dies allerdings nicht mehr der einzige Aspekt, der beachtet werden muss, wenn man sich mit vertrauensschaffenden Maßnahmen für seine Webseite beschäftigt. Insbesondere in der Zeit nach der NSA-Affäre werden auch Themen wie IT-Sicherheit und Datenschutz für viele User immer wichtiger.

Dieses E-Book soll Betreibern von Online-Shops zeigen, durch welche Maßnahmen sie gezielt die Vertrauenswürdigkeit ihrer Webseite verbessern können. Wenn es darum geht neue Besucher zu Käufern zu machen, gilt es jede mögliche Maßnahme zu ergreifen, die das Bedürfnis des Users nach Vertrauen befriedigen kann.

Inwiefern stimmen Sie den folgenden Aussagen zu?

Abb. 1: Einschätzungen von Online- Shops mit Gütesiegeln, 963 ⩽ n ⩽ 981 (Darstellung der Häufigkeiten; Skala: 1 = stimme überhaupt nicht zu bis 4 = stimme voll und ganz zu). **Quelle:** ECC-Handel, *www.ecckoeln.de*

KAPITEL 1:

Trust-Signale, die jede Ecommerce-Webseite braucht

Wie wichtig sind Ihnen folgende Punkte beim Online-Einkauf?

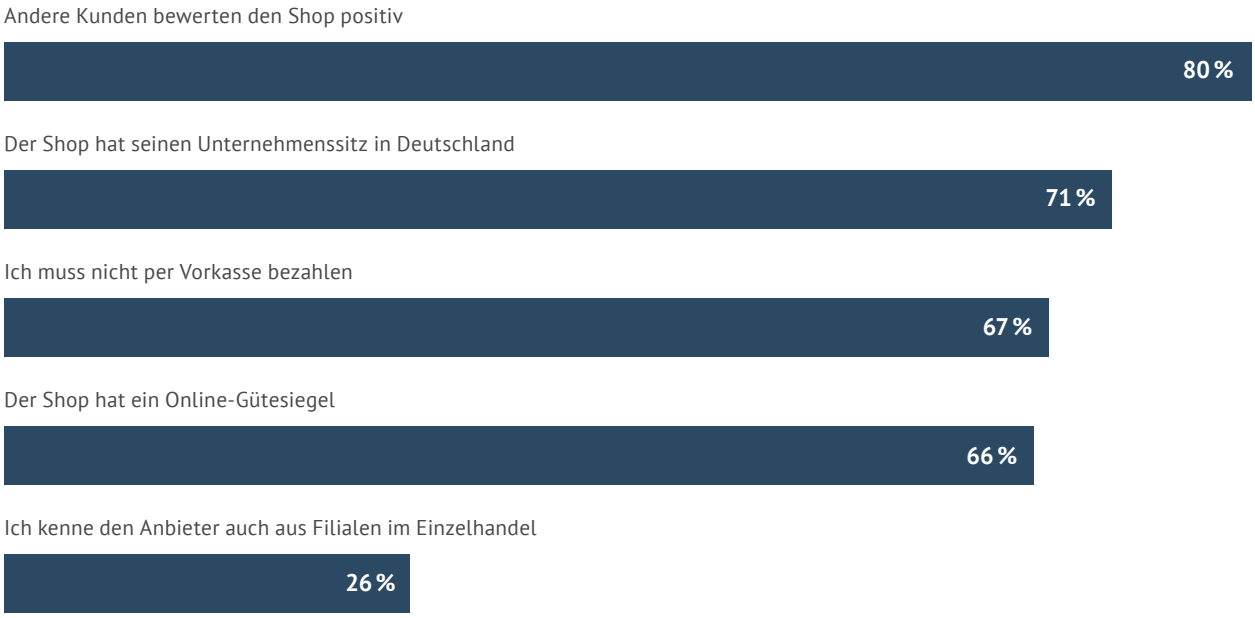

Abb. 2: Top2 auf einer Skala von 1 „sehr wichtig“ bis 5 „sehr unwichtig“. **Quelle:** Online-Käufer n – 1.026

KAPITEL 1.1:

Wieso Vertrauenssiegel für Online-Shops wichtig sind

Viele Verbraucher kennen das ungute Gefühl, wenn sie eine Kreditkarten- oder Kontonummer bei einem Online-Shop angeben müssen, bei dem sie noch niemals etwas gekauft haben. Der Wunsch vieler Verbraucher nach Sicherheit beim Online-Shopping ist groß. Viele Händler setzen deshalb auf Kundenbewertungsportale.

Heutzutage kann fast alles über das Internet gekauft werden, egal ob Lebensmittel, Unterhaltungselektronik oder Autos. Wer auf der Suche nach einem ganz bestimmten Artikel ist, kann sich vorher im Internet informieren, ob sich die Anschaffung lohnen wird. Mit Hilfe von Kundenbewertungsportalen wie eKomi liefern andere Nutzer Erfahrungen und Bewertungen und helfen Verbrauchern, ihre Kaufentscheidung zu erleichtern.

SHOPBEWERTUNGEN NUTZEN

Gerade für kleinere Online-Shops sind Shopbewertungen extrem wichtig. Mit Systemen wie eKomi ist es nicht nur möglich einzelne Produkte zu bewerten, sondern User können auch Erfahrungen über den gesamten Shop einsenden. Potentielle Kunden erfahren so sehr schnell, ob ein Shop seine Sendungen gut verpackt oder seine Bestellungen schnell bearbeitet.

Das Tool zur Kundenbewertung von eKomi kommt bei Kunden sehr gut an. eKomi-Bewertungen lassen sich ebenfalls in den Google-Shopping Ergebnissen und in den Google Adwords Werbeanzeigen anzeigen. Hier können die Sternchen für erhöhte Klickraten sorgen.

Zusätzlich gibt es auch die Möglichkeit, die Kundenbewertungen des eKomi-Tools in den organischen Suchergebnissen anzeigen zu lassen. Hierdurch werden in den organischen Suchergebnissen die Anzahl der Bewertungen und fünf Sternchen angezeigt.

Neben kurzen Ladezeiten, Übersichtlichkeit und vielen anderen Elementen vertrauenswürdiger Websites sind auch Online-Gütesiegel ein sehr wichtiges Werkzeug, wenn es um die Optimierung des Online-Shops geht. Dies gilt insbesondere für Warenkorbwerte ab 200€. Kombiniert man Siegel und Bewertungsfunktion, fließen gleich zwei sehr wichtige vertrauensbildende Elemente in euren Shop ein.

KAPITEL 1.2:

10 Tipps, mit denen Ihr Onlineshop vertrauenswürdiger wird

Um im Internet Kunden zu gewinnen und auch zu binden, reicht es nicht aus einfach nur eine Webseite zu erstellen. Es wird immer wichtiger Vertrauen zu schaffen und die User hierdurch zur Kontaktaufnahme oder zum Bestellen zu bewegen. Dieser Artikel listet die 10 wichtigsten Tipps auf.

1. AUSZEICHNUNGEN & GÜTESIEGEL

Sie sollten niemals mit externen Vertrauenssignalen geizen. Haben Sie Zertifikate oder Auszeichnungen erhalten oder verwenden Sie Gütesiegel wie eKomi, dann sollten diese prominent auf der Webseite eingebunden werden.

2. AKTUELLE INHALTE

Für eine erfolgreiche Kundengewinnung sind die Inhalte Ihrer Webseite extrem wichtig. Lassen sie Texte nicht von Praktikanten schreiben. Professionelle Texter sind immer eine gute Investition. Dies betrifft nicht nur den eventuell vorhandenen Blog, sondern auch sämtliche andere Inhalte wie die Texte auf Landing Pages, zur Verfügung gestellte Informationen über das Unternehmen oder Produktbeschreibungen.

Inhalte sollten nicht veraltet sein, sondern einen gewissen Mehrwert bieten. Wenn Sie keine Zeit haben die Inhalte auf Ihrer Webseite zu pflegen, ist es oft sogar ratsamer, keine zeitlich relevanten Informationen bereitzustellen.

3. KUNDENBEWERTUNGEN

Viele Menschen informieren sich vor dem Kauf eines Produktes über dessen Bewertung durch andere Käufer. Eine Umfrage des statistischen Bundesamts ergab, dass 56 % der Befragten Kundenbewertungen als wichtig oder sehr wichtig empfinden. Detaillierte Informationen zum Einfluss von Kundenbewertungen auf die Verkäufe und SEO Ihrer Webseite finden Sie auch hier.

4. FOTOS

Fotos sind ein extrem wichtiges Instrument, um Vertrauen aufzubauen. Dazu gehört neben einem sympathischen und authentischen Teamfoto auch Fotos von Ansprechpartnern und Verantwortlichen.

5. AUF FRAGEN UND WÜNSCHE DER KUNDEN EINGEHEN

Ein potentieller Kunde sollte immer sofort erkennen, was das Thema der Webseite ist. Entscheidend ist auch, ob er das Gesuchte dort finden kann. Extrem hilfreich ist auch zu zeigen, was der potentielle Kunde erhält, sofern er Kunde werden sollte. Informationen über Lieferzeiten, Nebenkosten und Garantien sind deshalb extrem wichtig und helfen dabei Vertrauen aufzubauen. Auch bietet es sich an, einen FAQ mit den häufigsten Fragen der Kunden auf der Webseite anzubieten.

6. EXTERNE LINKS

Viele Webseitenbetreiber setzen ungern externe Links, da sie Angst haben Kunden zu verlieren. Selbstverständlich sollten sie nicht auf die direkte Konkurrenz verlinken, dennoch ist es eine falsche Entscheidung überhaupt keine externen Links zu setzen. Ein paar gute, vertrauenswürdige externe Links sind absolut sinnvoll. Die Besucher Ihrer Webseite wissen hilfreiche, weiterführende Informationen, die einen Mehrwert bieten, sehr zu schätzen.

7. PRESSEBEREICH

Ein Pressebereich lohnt sich auch für kleinere Onlineshops. Neben der Möglichkeit, dass Presseverantwortliche sich hier ggf. Pressemitteilungen herunterladen können, bietet ein Pressebereich auch Potential für normale Nutzer. So kann man beispielsweise Zeitungsausschnitte oder Artikel aus Online-Medien in den Pressebereich mitaufnehmen. Das stärkt Ihre Authentizität und Vertrauenswürdigkeit.

8. ÜBERSICHTLICHKEIT/USABILITY

Die Übersichtlichkeit einer Webseite ist für Ihren Erfolg absolut wichtig. Die wichtigsten Informationen sollten sofort ins Auge springen - möchte der Nutzer mehr Informationen können diese auf Unterseiten bereitgestellt werden. Insbesondere die Navigation sollte nicht überladen sein und Begriffe enthalten, die die User kennen und verwenden.

9. VIDEOS

Der gezielte und richtige Einsatz von Videos auf Ihrer Webseite hat einen sehr positiven Einfluss auf das Kundenverhalten. Kurze und prägnante Erklärvideos eignen sich hervorragend, um Produkte, Dienstleistungen und Ihr Unternehmen vorzustellen. Sehen potentielle Kunden ihre Produkte in Aktion können sie deren Funktionalität besser verstehen. Das stärkt das Vertrauen und ist auch gut für die Conversion-Rate.

10. LIVE-CHATS

Durch einen Live-Chat können Sie die Lücke zwischen Ihren Kunden und sich selbst schließen. Live-Chats ermöglichen Ihnen, sich direkt mit Ihrem Kunden auseinanderzusetzen und können so Ihr Vertrauen gewinnen. Insbesondere in den USA bieten viele Onlineshops Live-Chats an.

Fazit: *Wenn Sie die oben genannten Tipps beachten und potentiellen Kunden eine übersichtliche, gut strukturierte Webseite mit vertrauenswürdigen, aktuellen Inhalten und allen benötigten Informationen zum Shop anbieten, werden nicht nur Ihre Verkaufszahlen steigen, sondern Ihre Webseite wird auch immer mehr als echte Marke wahrgenommen.*

KAPITEL 2:

IT-Sicherheit

KAPITEL 2.1:

Was ist https und wieso sollten Webseiten es verwenden?

WAS IST HTTP/HTTPS ÜBERHAUPT?

Das Hypertext Transfer Protocol (kurz HTTP) ist ein Protokoll, welches zur Übertragung von Daten genutzt wird. Den meisten Lesern wird HTTP bei der Nutzung des Internets begegnet sein, da das Protokoll hier verwendet wird, um Webseiten (Hypertext-Dokumente) aus dem World Wide Web (WWW) in einem Webbrowser zu laden. Da beim Protokoll HTTP in den Anfängen fast nur Inhalte von einem Anbieter (Webseite) zum User (Webseitenbesucher) transportiert wurden, fand dies ohne Verschlüsselung statt und war damit auch im Klartext lesbar. Mittlerweile nutzt fast jede Anwendung das Internet und sowohl Anbieter als auch Nutzer übertragen sensible Daten (Onlinebanking, Online-Kreditanfragen oder Showanwendungen über welche Bankverbindungsdaten zur Bezahlung übermittelt werden uvm.). Aus diesem Grund wurde ein ergänzender Standard, HTTPS (Hypertext Transfer Protocol Secure) zur verschlüsselten Übertragung entwickelt.

WELCHE VORTEILE BIETET HTTPS GEGENÜBER HTTP?

Der Vorteil bei der Nutzung von HTTPS liegt in der Verschlüsselung. Die Verschlüsselung stellt sicher, dass die Daten beim Besuchen einer Webseite zwischen dem Besucher der Webseite und dem Betreiber der Webseite verschlüsselt sind. Dies ist vor allem wichtig, sobald man auf der Webseite eventuell vertrauliche Informationen austauschen möchte. Wichtig ist hierbei nur, dass es sich hier um eine sogenannte Ende zu Ende Verschlüsselung handelt welche nur zwischen den beiden ausgehandelten Partnern eine sichere Kommunikation ermöglicht. Sollten Sie zum Beispiel einen Shop besuchen, um etwas online zu kaufen, dann ist eine verschlüsselte Verbindung extrem wichtig, da Sie in der Regel im Laufe des Bestellprozesses Ihre Adresse, eventuell Bankverbindung oder Kreditkartendaten übertragen. Bei einer HTTP Verbindung (Beispiel http://wwww.shop.de) könnte relativ einfach ein Dritter diese Daten abfangen und Sie gegebenenfalls als gestohlene Identität missbrauchen oder gar verkaufen. Die polizeiliche Kriminalstatistik weist für das Jahr 2013 insgesamt circa 64.000 “offiziell” gemeldete Onlinestraftaten aus. Privatpersonen in Deutschland entsteht den WISIND-Berechnungen (WISDN = Wirtschaftswissenschaftlicher Sicherheitsindikator für Deutschland) zufolge pro Jahr ein Schaden von rund 3,4 Milliarden Euro.

WORAUF MUSS BEI DER UMSTELLUNG VON HTTP AUF HTTPS GEACHTET WERDEN?

Bei der Nutzung des Internets gilt generell, dass man beim Einsatz von HTTP wie auch bei HTTPS nicht blind vertrauen darf. HTTPS

verwendet zur Verschlüsselung des Datenverkehrs ein Zertifikat (ähnlich Ihrem Ausweis). Dieses Zertifikat sollte von einem „vertrauenswürdigen“ Trustcenter (Vergabestelle von Zertifikaten) signiert sein und muss unbedingt gültig sein. Da ein Ausweis zur Feststellung der Identität genutzt wird, sollten Sie unbedingt die Echtheit prüfen. Dies können Sie indem Sie die Details des Zertifikates prüfen (klicken Sie mit der linken Maustaste auf das Schlosssymbol im Browser).

Stellen Sie sich vor, Sie planen zur Sicherung Ihrer Wertgegenstände den Einbau eines Türschlosses. Nur wenn sichergestellt ist, dass Ihre Schlüssel die einzigen sind, ist sichergestellt, dass Ihr Schloss die erhoffte Sicherheit bringt.

Daher setzten Sie zum Einen auf einen vertrauenswürdigen Hersteller, welcher durch verschiedene Nachweise glaubhaft versichert, dass Ihr Schloss und Ihr Schlüssel einzigartig und sicher ist. Dies gilt genauso für die bei HTTPS verwendeten Zertifikate. Nur wenn sichergestellt ist, dass dieses Schloss und die Schlüssel vertrauenswürdig sind, sollten Sie darüber kommunizieren. Sollten Sie eine Fehlermeldung des Browsers bekommen, dass die Identität/ Herkunft oder das Zertifikat nicht als vertrauenswürdig eingestuft ist, oder in den Zertifikatsdetails widersprüchliche Daten stehen, dann sollten Sie die Verwendung überdenken. Es könnte sich um einen Betrüger handeln und der Shop könnte nur zum Ziel haben, Sie um Ihr Geld zu erleichtern. Es könnte aber auch sein, dass ein Dritter versucht sich in Ihre Verbindung einzuklinken, um sensible Daten wie z.B. Bankdaten zu stehlen. In jedem Fall sollte der Betreiber der Webseite telefonisch oder per Email informiert und darauf aufmerksam gemacht werden - denn eventuell wurde er Opfer eines Hackers.

NICOLAI LANDZETTEL
Geschäftsführer Data-Sec

Data-Sec hat sich auf die IT-Sicherheit für mittelständische Unternehmen spezialisiert. Seit 2008 bietet das Unternehmen mit derzeit über 10 Mitarbeitern von der Auditierung, Konzeption, Installation bis hin zur laufenden Betreuung einen Rundumschutz an, der alle gesetzlichen Anforderungen erfüllt und alle wichtigen Risiken abwehrt. Als langjähriger Dell-Partner wurde Data-Sec 2014 der erste ‚Dell Premier Partner‘ im Networking und Security-Bereich aus Europa. Diesen Status erlangte Data-Sec nach mehrfachen Auszeichnungen als Partner des Jahres, unter anderem 2014 als ‚Enterprise-Partner des Jahres‘. Zu den Kunden zählen Unternehmen wie Ravensburger, Carhartt, Der Tagesspiegel und dennree. Partnerschaften bestehen außerdem mit Sophos, SafeNet, Sirrix, FTAPI, Imperva, Tripwire, Compumatica und wave.

Weitere Informationen unter www.data-sec.net

KAPITEL 2.2:

Welche Bezahlsysteme sollten Onlineshops anbieten?

Das Traumsofa oder die neuen Lieblingsschuhe sind im Internet oft nur einen Mausklick entfernt. Einkaufen im Internet ist um ein Vielfaches leichter: Man muss nicht mehr durch unzählige Geschäfte laufen, bis man den gewünschten Artikel gefunden hat. Es findet sich leichter ein Schnäppchen in der passenden Größe oder der passenden Auswahl.

Unzählige Online-Shops bieten hier eine riesige Auswahl an, bei denen man den gewünschten Artikel schon mit wenigen Klicks findet. Ob Amazon, Ebay, Zalando oder Buch.de. Waren im Internet sind schnell bestellt. Der Internethandel boomt. Ein Branchenriese verspricht sogar die bestellten Artikel noch am gleichen Tag auszuliefern.

Das Zahlen im Internet ist nicht nur bequem, sondern in den meisten Fällen auch sicher.

Sicher? Viele Tausend Onlineshops geben ihren Kunden die Möglichkeit, sich zwischen verschiedenen Zahlungssystemen zu entscheiden. Aufgrund des immer breiteren Angebotes ist es nicht ganz einfach, die verschiedenen Bezahlverfahren auseinanderzuhalten. Es ist daher sinnvoll, sich einen Überblick über die Eigenschaften sowie die Vor- und Nachteile der beliebtesten Systeme zu verschaffen.

ERST DAS GELD UND DANN DIE WARE!

Dies ist das Prinzip bei der weit verbreiteten Kreditkartenzahlung, die jedoch in keinem Online-Shop fehlen sollte.

Vorteil: Der Onlinehandel wird schnell abgewickelt.

Nachteil: Es fallen Gebühren der Zahlungsabwicklung an und bei einer Reklamation oder Nichtgefallen muss das Geld vom Händler zurückgefordert werden. Es kann nicht sichergestellt werden, wie der Händler mit diesen vertraulichen Zahlungsangaben umgeht.

Empfehlenswert: Ja

Ebenfalls geht man mit der Vorkasse ein finanzielles Risiko ein, bevor man die Ware zu Gesicht bekommt:

Vorteil: Kein Vorteil

Nachteil: Der Handel wird durch die Überweisung, bis das Geld beim Händler ankommt (meistens 2 bis 3 Tage), verzögert. Nicht selten dauert so eine Transaktion 1 bis 2 Wochen. Vorsicht ist geboten, da eine Überweisung nicht ohne weiteres rückgängig gemacht werden kann. Auch hier muss bei einer Reklamation das Geld vom Händler zurückgefordert werden.

Empfehlenswert: Nein

Auch per Sofortüberweisung (Onlineportal) bekommt man die Ware nicht erst, bevor eine Bestätigung der Zahlungsanweisung beim Onlineshop ist. Hier wickelt ein externer Dienstleister die Transaktion vom normalen Bankkonto ab.

Vorteil: Der Onlinehandel wird schnell abgewickelt.

Nachteil: Bei dieser Zahlungsart gibt der Nutzer auf der jeweiligen Shopseite zunächst die Bankleitzahl und anschließend den eigenen Namen und die Kontonummer ein. Abgeschickt wird die Überweisung nach Eintippen der PIN und einer TAN. Somit hat der Anbieter theoretisch vollen Zugang zu allen Kontoständen und Kontobewegungen. Zudem können Haftungsfragen im Schadensfall kompliziert werden. Auch hier muss bei einer Reklamation das Geld vom Händler zurückgefordert werden.

Empfehlenswert: Ja (mit Vorsicht)

Bei der Bezahlung per Nachnahme bekommt man die Ware eigentlich auch erst zu Gesicht, wenn man bereits bezahlt hat. Bezahlt wird die Ware jedoch nicht schon bei der Bestellung, sondern später beim Eintreffen des Paketes an den Überbringer.

Vorteil: Der Onlinehandel wird schnell abgewickelt.

Nachteil: Die Ware kann nicht direkt überprüft werden, da der (Post)bote das Paket erst beim Zahlungsempfang heraus gibt. Auch hier muss bei einer Reklamation das Geld vom Händler zurückgefordert werden und es fallen neben den Versandkosten hohe Zusatzgebühren von meist über fünf Euro an.

Empfehlenswert: Ja (mit Vorsicht)

Prepaid-Online-Zahlungsmittel wie paysafecard oder Ukash werden als alternative Bezahlsysteme im Internet immer beliebter. Prepaid-Onlinebezahlsysteme funktionieren ähnlich wie eine Wertkarte für Mobiltelefone die man ebenfalls an den bekannten Verkaufsstellen (wie etwa Kioske, Tankstellen oder Supermärkte kaufen) kann.

Vorteil: Man kann auch kleine Beträge bei Online-Käufen bequem bezahlen, ohne dabei private Daten wie Name oder Kontoverbindung angeben zu müssen. Der Onlinehandel wird schnell abgewickelt.

Nachteil: Kommen Betrüger im Besitz von PINs, die der Kunde für seine Käufe nutzt, können sie selbst damit im Internet auf Shoppingtour gehen. Häufig werden die PINs auch im großen Stil durch Betrügereien und Erpressungen erlangt und am Ende „ausgecasht“, also wieder in Bargeld umgewandelt.

Empfehlenswert: Ja (jedoch nur für kleinere Beträge)

Es geht auch anders:

ERST DIE WARE UND DANN DAS GELD!

In vielen Online-Shops kann das Geld auch über Bezahlsystem-Anbieter wie zum Beispiel PayPal, Click & Buy (Deutsche Telekom) oder Moneybookers überwiesen werden. Bezahlsysteme vermitteln zwischen Händler und Käufer.

Allerdings müssen Verbraucherinnen und Verbraucher bei diesen Bezahldiensten ebenfalls ein Kundenkonto einrichten und sicherstellen, dass niemand Zugriff auf ihre Zugangsdaten hat. Unterliegen der neuen Regelung *„Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)“* für Zahlungsdienstleister in Deutschland und Europa.

Vorteil: Der Onlinehandel wird schnell abgewickelt. Kontodaten werden nicht an den Online-Händler übermittelt. Alle Daten der Transaktion bleiben beim Bezahlsystem-Anbieter. Bei Reklamation muss das Geld nicht vom Händler teuer zurückgeholt werden.

Nachteil: hohe Phishing-Attacken und Abbruch der Transaktion durch hohe Fehlalarme des automatischen Betrugserkennungssystems.

Empfehlenswert: Ja

Ähnlich funktioniert das von der deutschen Kreditwirtschaft (Bafin) herausgebrachte Giropay Verfahren auf Basis des Online Banking.

Teilnehmende Banken sind u. a. die Sparkassen, Volks- und Reifeisenbanken und die Postbank. Der Händler erhält unmittelbar nach erfolgreicher Zahlung eine Zahlungsgarantie der Bank und kann somit Waren sofort und ohne Risiko zur Verfügung stellen. Ebenfalls unterliegt Giropay der neuen Regelung *„Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)“* für Zahlungsdienstleister in Deutschland und Europa.

Vorteil: Der Onlinehandel wird schnell abgewickelt. Kontodaten werden nicht an den Online-Händler übermittelt. Alle Daten der Transaktion bleiben beim Bezahlsystem-Anbieter.

Nachteil: hohe Phishing-Attacken. Eine einmal getätigte Zahlung kann nicht zurückgefordert werden. Nicht jede Bank bietet diese Zahlungsoption an.

Empfehlenswert: Ja

Die sicherste Zahlungsart ist der Kauf auf Rechnung. Aufgrund des finanziellen Risikos bieten aber nicht alle Online-Shops diese Zahlungsmöglichkeit an.

Vorteil: Der Onlinehandel wird schnell abgewickelt. Bei Reklamation muss das Geld nicht vom Händler teuer zurückgeholt werden. Es werden keine Bankdaten an den Anbieter übermittelt.

Nachteil: Wird meist erst nach einer Erstbestellung oder einer Schufa-Auskunft akzeptiert.

Empfehlenswert: Ja

Bezahlverfahren – Nutzung im Internet in Deutschland 2012 bis 2015

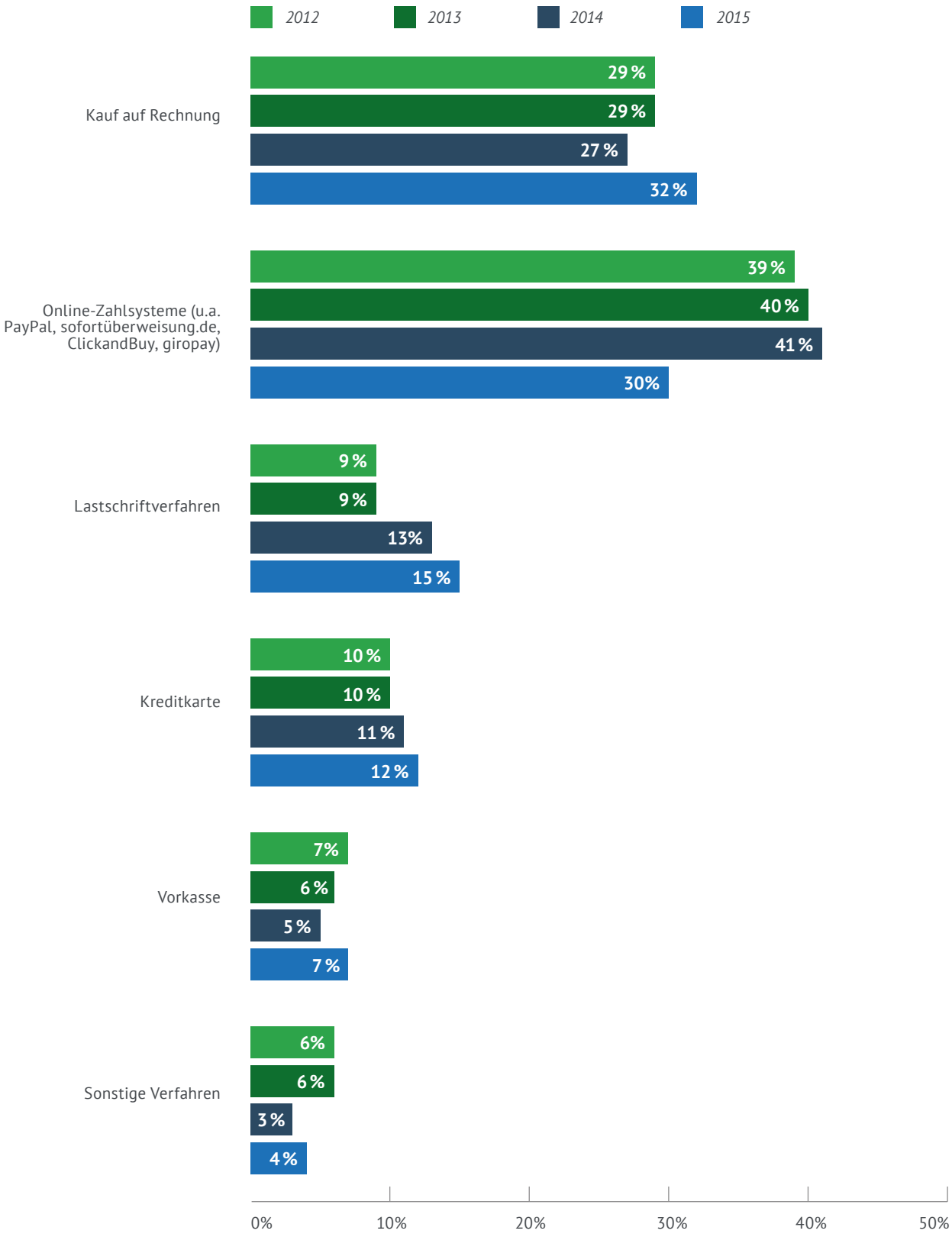

Abb. 3: Anteil der Befragten, die folgende Bezahlverfahren im Internet schon einmal genutzt haben in den Jahren 2012 bis 2015.
Quelle: © Statista 2015

NEUE SICHERHEITS-MASSNAHMEN

Um das Vertrauen der Verbraucher beim Zahlen im Internet an sich zu stärken, gelten ab den 05. November 2015 neue **Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)** für Zahlungsdienstleister in Deutschland und Europa.

Wichtiger Eckpunkt bei der Umsetzung ist eine sichere Authentifizierung für Internetzahlungen. Dazu stehen zwei verschiedene Merkmale aus drei möglichen Kategorien zur Verfügung. Zur ersten Kategorie zählt beispielsweise ein Passwort, ein Code oder eine PIN. In einer weiteren Kategorie werden Gegenstände genannt, die nur der Nutzer besitzt, zum Beispiel das Mobiltelefon oder ein TANGenerator. Die Eigenschaften des Nutzers, wie etwa Fingerabdruck, die Stimme oder der Pulsschlag, bilden die dritte Kategorie. Um Missbrauch und Betrug zu verhindern, müssen sich Kunden zukünftig doppelt identifizieren und mindestens zwei Merkmale aus den drei möglichen Kategorien erfüllen.

Im Online-Handel sind vor allem die Kreditkartenzahlung sowie Überweisungen betroffen, wenn diese etwa über giropay oder Sofort-Überweisung abgewickelt werden. Nicht betroffen sind der Kauf auf Rechnung, der Ratenkauf und die Zahlung per Lastschrift in seiner derzeit gängigen Form. Ausgenommen von der starken Kundenauthentifizierung sind Bezahlmethoden, die als sicher gelten. Zu nennen sein soll hier Paypal. Zahlungen unter 30 Euro sind von der neuen MaSi ausgenommen.

KÜNFTIGES PAYMENT-VERHALTEN

Traditionelle Zahlmöglichkeiten wie das Lastschriftverfahren und die Kreditkarte sind bereits unter Druck geraten. Längst können die etablierten Verfahren nicht mehr die heutigen Kundenansprüche erfüllen: Zahlen zu jeder Zeit, an jedem Ort und mit jedem Gerät. Des Weiteren wird E-Commerce zunehmend durch den M-Commerce ersetzt. Somit steigt der Bedarf an mobilen Bezahlmethoden, die

Kunden die Freiheit geben, unabhängig von der Situation eine Zahlung auszulösen. Online-Händler müssen sich neuen Vertriebs- sowie Vermarktungsmöglichkeiten öffnen und sich auf das zunehmend technisch versierte Verbraucherverhalten einlassen, wenn sie nicht Gefahr laufen wollen, Marktanteile zu verlieren.

ABSCHLIESSENDE VORBEUGENDE IT-SICHERHEITSMASSNAHMEN

Auf jedem System sollten sowohl ein Antivirenschutzprogramm als auch eine Firewall installiert sein. Das Betriebssystem sowie alle eingesetzte Software sind stets auf dem aktuellen Stand zu halten und Aktualisierungen sowie Sicherheitspatches (Updates) sollten umgehend nach Erscheinen installiert werden. Eine regelmäßige Datensicherung macht Nutzer weniger angreifbar – etwa für Erpressungsversuche durch Ramsomware.

E-Mail-Anhänge oder Web-Links in E-Mails, in sozialen Netzwerken oder Chats sollten nur mit besonderer Vorsicht geöffnet werden, auch wenn sie von bekannten Quellen stammen. Gegebenenfalls sollte beim Absender nachgefragt werden. Empfehlenswert ist ein Administrator-Benutzerkonto sowie ein Benutzerkonto mit eingeschränkten Rechten um einem potenziellen Angreifer unter Umständen den Zugriff auf sämtliche Daten nicht zu ermöglichen. Für alle Online-Dienste sollten sichere Passwörter (mind. 8 Zeichen bestehend aus Groß/Kleinbuchstaben und Sonderzeichen) gewählt werden, die regelmäßig gewechselt werden. Für verschiedene Dienste sollte niemals das gleiche Passwort verwendet werden.

KARSTEN ZIMMER
Dipl. Informatiker, EDV-Sachverständiger & IT Forensiker

Der Dipl. Fachinformatiker ist Spezialist für Datensicherheit in der Unternehmenskommunikation genauso wie in sozialen Netzwerken. Außerdem arbeitet er in Sachen IT und Datensicherheit eng mit dem Bundeskriminalamt zusammen. Seine Vorträge sind eine Mischung aus interessanter Wissensvermittlung über alle Formen des Datendiebstahls, der Bespitzelung und des Betrugs angereichert mit praktischen Beispielen bis hin zur Demonstrationen von erstaunlichen Effekten. Bei Aufdeckungen von Industriespionage ermittelt er Hackerangriffe ebenso wie kürzlich auch im deutschen Bundestag.

Weitere Informationen unter www.csi-menden.de

KAPITEL 3:

Datenschutz

Wie stark vertrauen Internetnutzer der Wirtschaft allgemein in Bezug auf ihre persönlichen Daten im Netz?

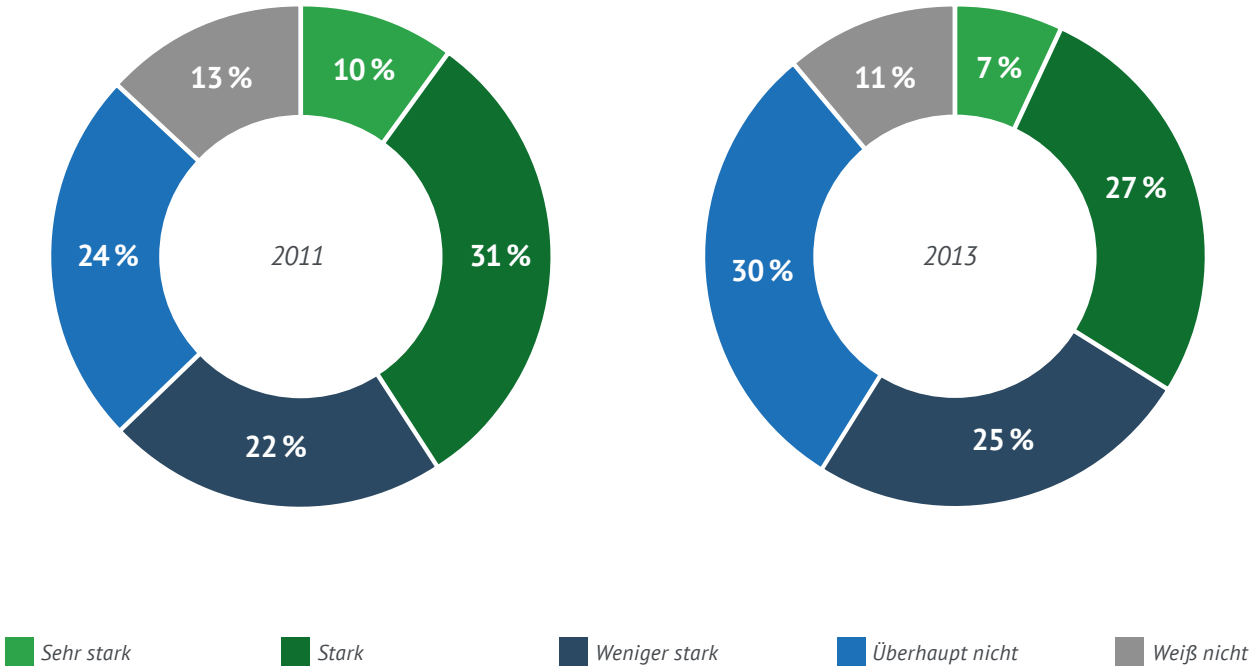

Abb. 4: Basis: Internetnutzer. **Quelle:** ARIS

KAPITEL 3.1:

Datenschutz für Onlineshops – worauf Sie als Händler achten müssen

Datenschutz und die damit verbundenen Pflichten spielen auch für Onlinehändler eine große Rolle. Bei jedem Kauf in einem Onlineshop fallen Kundendaten an: Name, Adresse, E-Mailadresse, Kreditkartenummer usw. Der Datenschutz für Internethändler und der Umgang mit den Kundendaten sind im Telemediengesetz (TMG) geregelt. Danach ist der Kunde immer darüber zu unterrichten, was datenschutztechnisch im Onlineshop passiert. In bestimmten Fällen ist außerdem die vorherige Einwilligung des Kunden zur Datenerhebung und –Verwendung erforderlich.

WAS DROHT BEI VERSTÖSSEN?

Die Verletzung datenschutzrechtlicher Pflichten kann zum einen nach neuester Rechtsprechung abgemahnt werden. So entschied das Oberlandesgericht Hamburg, dass das Fehlen einer korrekten Datenschutzinformation wettbewerbswidrig ist (Urteil vom 27.6.2013, Az. 3 U 26/12). Zum anderen besteht bei Verstößen gegen die Regelungen des TMG die Möglichkeit der Verhängung von Bußgeldern bis zu 50.000 € durch die Datenschutzbehörden. Bei Verstößen gegen das Bundesdatenschutzgesetz (BDSG) drohen teilweise sogar Bußgelder bis zu 300.000 €.

WAS HEISST „DATENSCHUTZ-INFORMATION“ UND WIE MUSS DAS UMGESETZT WERDEN?

Nutzer von Internetseiten sind immer über eine „Datenschutzinformation“ zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung ihrer personenbezogenen Daten zu unterrichten. Diese Verpflichtung gilt auch für Onlineshops. Dazu muss der Internethändler eine umfassende und leicht auffindbare Information für den Kunden in den Shop platzieren. Diese Datei muss alle Informationen über Art, Umfang und Zweck der Erhebung, Verwendung und Verarbeitung der Nutzer- und Kundendaten enthalten. Die Seite sollte „Datenschutzinformation” oder “Datenschutz” heißen.

WANN BENÖTIGEN HÄNDLER DAS EINVERSTÄNDNIS IHRER KUNDEN FÜR DIE DATENERHEBUNG UND -NUTZUNG?

Nach dem TMG dürfen personenbezogene Daten von Nutzern oder Kunden nur dann ohne deren Einwilligung erhoben und verwendet werden, sofern das gesetzlich erlaubt ist. Diese gesetzliche Erlaubnis besteht beispielsweise bei Bestandsdaten und Abrechnungsdaten, die unerlässlich sind für die Abwicklung und Abrechnung des Internet-Geschäftes. Damit dürfen zu diesem Zweck etwa der Name, die Adresse und die Zahlungsinformationen bei einer Bestellung gespeichert werden. Das gilt aber nur zum Zweck dieses jeweiligen Geschäftes, also zum Beispiel der einmaligen Abwicklung des Kaufs. Das bedeutet: Daten, die der Händler ausschließlich zur Abwicklung einer Bestellung erhebt und nutzt, dürfen ohne besondere Einwilligung des Kunden erhoben und gespeichert werden. Sollen die Daten jedoch für andere Zwecke genutzt werden (z.B. Verwendung für Werbemails an den Kunden, Einrichtung eines Kundenkontos), ist das vorherige Einverständnis des Kunden dazu erforderlich. Trägt der Kunde also seine Daten in ein Bestellformular ein, muss er für die Verwendung dieser Daten zur Abwicklung dieser Bestellung nicht extra einwilligen. Sollen die Daten auch für Werbemailings oder eine dauerhafte Kundenregistrierung gespeichert werden, ist dazu im Formular das Einverständnis einzuholen, etwa durch Anklicken eines entsprechenden Hinweises: „Bitte schicken Sie mir den Newsletter zu. Ich kann mich jederzeit wieder abmelden.“, „Ich möchte ein Kundenkonto einrichten.“

FLORIAN DECKER

Fachanwalt für Informationstechnologierecht (IT-Recht)

Rechtsanwalt Florian Decker verfügt als Fachanwalt für IT-Recht insbesondere über hervorragende Kenntnisse im IT-Projektgeschäft und dem Datenschutzrecht. Zu den von ihm betreuten Mandanten zählen unter anderem Softwarehäuser, Agenturen und E-Commerce-Plattformen. Darüber hinaus ist er als externer Datenschutzbeauftragter tätig. Als Referent ist Rechtsanwalt Decker regelmäßig bei fachbezogenen Veranstaltungen vertreten. Dazu zählen unter anderem Vorträge bei IT-Events, Industrie- und Handelskammern, Messen und Workshops. In der Vergangenheit war er bereits als Lehrbeauftragter an der FH Worms tätig.

Weitere Informationen unter www.res-media.net

KAPITEL 3.2:

Transparenter Umgang mit personenbezogenen Daten für Onlineshops

Online-Shops müssen ihre Kunden über die Erhebung personenbezogener Daten informieren. Nur so können diese später auch ihre Ansprüche aus dem Bundesdatenschutzgesetz geltend machen: Die Betroffenen haben grundsätzlich einen Anspruch auf Auskunft, Berichtigung, Löschung und Sperrung der Daten. Auf die einzelnen Ansprüche und die Voraussetzungen für ihre Durchsetzung, wollen wir im Folgenden eingehen.

DAS RECHT AUF AUSKUNFT DER ERHOBENEN DATEN

Die Betroffenen können von dem Unternehmen verlangen, dass ihnen genaue Auskunft darüber erteilt wird, welche Daten gespeichert und weitergegeben wurden. Zudem ist auch der Zweck der Speicherung und Weitergabe anzugeben. Die Auskunft ist in der Regel schriftlich zu erteilen. Kosten dürfen dem Betroffenen dafür in der Regel nicht auferlegt werden. Ein Auskunftsrecht besteht allerdings nicht in den Fällen, in denen eine Benachrichtigungspflicht ausnahmsweise nicht besteht, beispielsweise wenn die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist).

HINWEIS AUF DAS WIDERSPRUCHSRECHT

Der Betroffene ist in jedem Fall auf sein Widerspruchsrecht hinzuweisen. Er kann beispielsweise in der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung widersprechen. In diesem Fall ist eine Verarbeitung der Daten zu diesem Zweck unzulässig.

DIE BERICHTIGUNG UND LÖSCHUNG ODER SPERRUNG VON DATEN IST ZWINGEND

Personenbezogene Daten sind zu berichtigen, wenn sie fehlerhaft sind und zu löschen, wenn ihre Speicherung unzulässig war oder der Zweck der Datenverarbeitung bereits erfüllt wurde und die Daten somit nicht mehr gebraucht werden. Es gilt das Prinzip der Datensparsamkeit.

In Fällen, in denen eine Löschung der Daten nicht in Frage kommt, etwa weil der Aufwand für eine Löschung besonders hoch wäre oder gesetzliche Aufbewahrungsfristen bestehen, kommt eine Sperrung in Betracht. Die gesperrten Daten dürfen ohne Einwilligung der Betroffenen dann grundsätzlich nicht mehr übermittelt werden.

Missachtet der Online-Shop die Rechte seiner Kunden, kann er verpflichtet werden dem Kunden Schadensersatz zu zahlen. Betroffene können sich im Fall einer Verletzung ihre Datenschutzrechte an den zuständigen Landesdatenschutzbeauftragten wenden.

DER DATENSCHUTZ-BEAUFTRAGTE

Um zu verhindern, dass Online-Shops nicht in die Rechtsfalle tappen, hilft ein betrieblicher, interner oder externer Datenschutzbeauftragter. Unternehmen, die personenbezogene Daten automatisiert verarbeiten und dafür mindestens 10 Personen ständig beschäftigen, sind verpflichtet einen solchen Beauftragten für den Datenschutz schriftlich zu bestellen. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit mindestens 20 Personen beschäftigt sind. In allen anderen Fällen ist die Beauftragung eines Datenschutzbeauftragten optional.

Der Datenschutzbeauftragte hat die Aufgabe auf die Einhaltung des Bundesdatenschutzgesetzes einzuwirken. Das heißt in der Praxis, dass dieser nicht selbst in die Geschäftspraxis eingreift, sondern beratend tätig ist und die Abläufe kontrolliert. Er macht Verbesserungsvorschläge, setzt diese aber nicht selbstständig um. Eine besonders wichtige Rolle spielt der Datenschutzbeauftragte daher im Hinblick auf die präventive Arbeit. Er kann die Geschäftsführung und die Mitarbeiter schulen, sodass erst gar keine Verletzung des Datenschutzrechtes entsteht.

> ***Achtung:*** *Der Datenschutzbeauftragte muss in gewisser Weise unabhängig sein. Das heißt, dass die Geschäftsführung nicht selbst die Kontrollaufgaben übernehmen kann.*

Ob ein interner oder externer Datenschutzbeauftrage bestellt wird, macht aus datenschutzrechtlicher Sicht keinen Unterschied. Der Vorteil eines externen Datenschutzbeauftragten ist jedoch zweifelsohne die größere Objektivität, die dieser mitbringt. Ein interner Mitarbeiter könnte geneigt sein nicht so hart durchzugreifen – mit teuren Folgen für das Unternehmen. Bei einem Verstoß gegen das Datenschutzgesetz ist die Verhängung von Ordnungsgeldern bis 300.000,- EUR möglich.

CHRISTIAN SOLMECKE

Rechtsanwalt für Medienrecht und IT-Recht

Christian Solmecke hat sich als Rechtsanwalt und Partner der Kölner Medienrechtskanzlei WILDE BEUGER SOLMECKE auf die Beratung der Internet und IT-Branche spezialisiert. So hat er in den vergangenen Jahren den Bereich Internetrecht/E-Commerce der Kanzlei stetig ausgebaut und betreut zahlreiche Medienschaffende, Web 2.0 Plattformen und App-Entwickler.

Weitere Informationen unter www.wbs-law.de

eKomi
The Feedback Company

Pressekontakt

eKomi The Feedback Company
Carrie Wick, *Head of Global PR & Communications*
Markgrafenstraße 11
10969 Berlin, Deutschland

Telefon: +49 (0)30 200 04 44 - 814
E-Mail: cwick@ekomi-group.com

ekomi.de