Wettbewerbsfaktor: Kundenvertrauen

Mit Datenschutz und Datensicherheit punkten

Die Welt des Kundenservice im Versandhandel und e-Commerce war bis dato über alle Service-Kanäle hinweg von Performance, Qualität, Flexibilität und Kostenoptimierung geprägt. Die optimale Ausrichtung dieser Stellschrauben war für viele Unternehmen der Garant für erfolgreichen Service. Doch in jüngster Zeit bewegt die Sicherung personenbezogener Daten den Kundenservice und viel mehr noch die Kunden.

Während Datenschutz und Datensicherheit in der Vergangenheit für viele Unternehmen eher eine gesetzlich vorgegebene Pflichtübung waren. So erhielten diese Themen in den letzten Monaten immensen Bedeutungszuwachs, so dass man hier mittlerweile von einem Wettbewerbsfaktor sprechen muss.

Sicherheit neu gedacht

Entscheidend dafür sind drei Entwicklungen. Die erste wurde durch ein Gerichtsurteil des Europäischen Gerichtshof (EuGH) ausgelöst. Während es in der Vergangenheit aufgrund von bilateralen Abkommen wie Safe Harbor mehr oder weniger unerheblich war, ob die Speicherung der Kundendaten auf dem europäischen oder amerikanischen Kontinent erfolgte, veränderte sich dies aufgrund des betreffenden EuGH-Urteils im Oktober letzten Jahres. Seitdem besteht nur noch Rechtssicherheit für die Datenspeicherung auf deutschen Servern – betrieben von deutschen Unternehmen. Den transatlantischen Datenverkehr und das Nachfolgeabkommen Privacy Shield beäugen Datenschützer weiter kritisch – Edward Snowden und die NSA-Affäre lassen grüßen.

© iStock, 2012

Die zweite Entwicklung erfolgte mit der Verabschiedung der Europäischen Datenschutzgrundverordnung im Dezember letzten Jahres. Auch wenn noch abzuwarten bleibt, wie die Datenschutzbehörden diese Verordnung auf nationaler Ebene auslegen werden, so ist aber heute schon gewiss, dass ihre Einführung deutliche Veränderungen mit sich bringen wird – dies gilt insbesondere auch bei den Strafmaßen und den damit verbundenen Bußgeldern.

Die dritte Entwicklung betrifft die Cyber-Kriminalität in Quantität als auch Qualität. Von der Cyber-Attacke auf SWIFT über die Zentralbank von Bangladesch – dem beinahe größten Bankraub der Geschichte – sowie den Diebstahl von über 100 Millionen Nutzerdaten bei LinkedIn bis hin zum Raub von 56 Millionen Kreditkarteninformationen und 53 Millionen E-Mail-Adressen beim US-Handelsunternehmen The Home Depot: Cyber-Kriminalität ist allgegenwärtig. Gelegenheit macht eben Diebe – dazu zählen Kleinkriminelle und organisierte Kriminalität ebenso wie staatliche Institutionen. Die Player und Interessen in diesem „Geschäft" sind vielfältig.

Fakten schaffen - Vertrauen verdienen

„Auch bei „König Kunde" besteht bereits ein Bewusstsein. Laut einer aktuellen repräsentativen Umfrage von Forsa hegen 38 Prozent der Online-Käufer den Verdacht, dass ihre Kontaktdaten nach Eingabe in die Hände Dritter fallen könnten und rund fünf Prozent geben an, dass ihre Zahlungsinformationen bereits missbraucht worden sind. Da wundert es nicht, dass 62 Prozent nicht glauben, dass ihre persönlichen Daten bei den Online-Shops sicher sind. Die Konsequenz: Im Falle eines Datenverlustes oder Datenmissbrauchs würden 72 Prozent der deutschen Online-Käufer nicht mehr im betreffenden Shop einkaufen und ihren Freunden und Familien ebenfalls vom Einkauf abraten.

Entwicklungen dieser Art müssen jedem Kundenverantwortlichen zu denken geben. Das weiß auch Dr. Benjamin Helbig, CIO bei walter services. Der Pionier im Customer Services und Anbieter von High-Security-Cloud-Lösungen hat seit fast 40 Jahren Erfahrung im Umgang mit Kundendaten. „Wir setzen auf eine Kombination an Sicherheitsmaßnahmen zum Schutz des firmeneigenen Netzes sowie den Kundendaten unserer Auftraggeber. In der heutigen Geschäftswelt, setzt alles auf Big Data, häufig ohne Abwägung von Nutzen und Risiken für Unternehmen wie Privatleute. Maßnahmen zum Schutz und zur Sicherung personenbezogener Daten sind daher unabdingbar, werden aber offenbar noch immer viel zu lax gehandhabt", so Helbig. „Ist das Vertrauen erst einmal enttäuscht, dann wird es für die Händler schwierig geschädigte Kunden zurückzugewinnen. Aus diesem Grund empfiehlt es sich Systeme und Dienstleister auf Sicherheitslücken zu überprüfen und gegebenenfalls nachzurüsten. Hier bieten unabhängige Zertifizierungen, wie bspw. das PCI-DSS-Siegel für die Bearbeitung von Kreditkartenzahlungen, Orientierungshilfe für die Unternehmen."

walterservices.com