

Kunden-Info

Online-Bezahlverfahren sind sicher



Heute sind Online-Zahlungssysteme für Online-Shops sehr sicher und unterliegen strengen Kontrollen von Seiten der Banken, Kreditkarten-Unternehmen und Finanzinstitute. Die geltenden Sicherheitsstandards im elektronischen Zahlungsverkehr sind die sichersten weltweit.

Schon seit es Online-Zahlungsverfahren gibt, werden mögliche Gefahren und Risiken durch intelligente Sicherheitsmechanismen nahezu ausgeschlossen. Spezielle Gremien, Institute und Firmen arbeiten kontinuierlich an Sicherheitsstandards und -lösungen für die Nutzung sensibler Daten im Internet. Diese Standards und Verfahren werden heute von allen seriösen Unternehmen eingesetzt, die im Internet mit sensiblen Daten arbeiten. Diese modernen Standards und Verfahren verwendet auch Computop beim Betrieb seiner Online-Zahlungsplattform Paygate und kann so eine maximale Datensicherheit für Internetshops und Käufer bei der Bezahlung sicherstellen.

Die heute gebräuchlichsten Verfahren und Standards im elektronischen Geldverkehr sind SSL- und Blowfish-Verschlüsselungen sowie die Regularien von PCI DSS (Payment Card Industry Data Security Standard).

SSL-Verschlüsselung

Bei der Bezahlung in Online-Shops werden Kunden kurzfristig auf die Server des Online-Payment-Dienstleisters Computop umgeleitet. Hier erfolgt die eigentliche Zahlung. Damit die Daten, wie beispielsweise die Kreditkartennummer, absolut sicher über das Internet übertragen werden, verwendet Computop durchgängig eine SSL-Verschlüsselung (Secure Socket Layer). Dabei werden die Daten mit einem Code verschlüsselt und können ohne entsprechende Entschlüsselungsalgorithmen nicht gelesen werden. Die bei Computop eingesetzte SSL-Verschlüsselung mit 128 Bit hat 340.282.366.920.938.000.000.000.000.000.000 verschiedene Kombinationsmöglichkeiten und kann daher von Unbefugten nicht entschlüsselt werden.

Blowfish-Verschlüsselung

Zusätzlich zur Sicherheit durch SSL werden alle Daten und Formulare im Computop Paygate per Blowfish verschlüsselt. Ein Vorteil von Blowfish ist seine variable Schlüssellänge von 32 bis zu 448 Bits, die eine sehr hohe Sicherheit bietet. Blowfish wurde 1994 zum ersten Mal vorgestellt und konnte bis heute nicht geknackt werden.

PCI Data Security Standard

Damit die Zahlungsdaten von Kunden nicht nur auf ihrem Weg durch das Internet sondern auch in den

Datenbanken aller am Zahlungsverkehr Beteiligten sicher vor einem unberechtigten Zugriff sind, unterliegen alle seriösen Plattformen für Online-Zahlungsverfahren den strengen Regularien von PCI DSS. Dieser Sicherheitsstandard wird von einem Gremium beständig weiter entwickelt und überwacht. Zu den Mitgliedern des Gremiums zählen unter anderem American Express, Mastercard und Visa.

Handelsunternehmen und Dienstleister, die Kreditkartentransaktionen speichern, übermitteln oder abwickeln müssen seit einigen Jahren diese Regelungen erfüllen. Halten sie sich nicht daran, können Strafgebühren verhängt, Einschränkungen ausgesprochen oder ihnen letztlich die Akzeptanz von Kreditkarten untersagt werden. Mit diesem Sicherheitsstandard werden auch die Server und die Sicherheit von Daten auf Festplatten geregelt. PCI stellt sicher, dass nirgendwo Zahlungsdaten von Käufern gelesen oder abgefangen werden können. Computop ist gemäß PCI DSS zertifiziert und wird in regelmäßigen Abständen immer wieder erneut geprüft. Die Zertifizierung beleuchtet dabei gleichermaßen technische wie organisatorische Aspekte und betrifft deshalb Themen wie Firewall-Konfiguration und Datenverschlüsselung ebenso wie Zugandskontrolle und Rechtezuordnung. Zusätzlich zu



Online bezahlen mit Sicherheit.

SSL, Blowfish und den Vorgaben von PCI DSS nutzt Computop zusätzliche Sicherheitsmechanismen zur Betrugsprävention und geht damit weit über die üblichen Standards hinaus. Damit können Kunden zu jeder Zeit darauf vertrauen, dass ihre Daten während der Online-Bezahlung im Internet sicher und für Dritte unlesbar übertragen werden.

Shop-Sicherheit bietet keine Garantie für PC-Datenklau

Obwohl die Sicherheit bei Zahlungsverfahren in deutschen Online-Shops quasi garantiert werden kann, gibt es immer wieder Fälle, wo ein Missbrauch von Kreditkartendaten im Internet geschieht. Die häufigste Ursache dafür sind Trojaner auf den PC-Systemen der Einkäufer. Trojaner sind kleine, unbemerkt eingeschleuste „Programme“, die spezielle Daten wie Kennwörter, Kreditkarten- oder Transaktionsnummern (TAN) be-

reits auf dem PC bei der Eingabe durch den Einkäufer „abgreifen“ und unbemerkt via Internet an eine bestimmte Adresse senden.

Wenn Trojaner auf einem PC ihr Unwesen treiben, sind die Sicherheitsmechanismen der Online-Shops und Zahlungssysteme machtlos und können demzufolge auch keine Garantie für diesen Datenklau gewähren. Daher ist für jeden Einkäufer im Internet ein guter Schutz vor Viren, Trojanern und Würmern heute oberstes Gebot. Diesen Schutz kann ein Anwender inzwischen leicht durch den Einsatz handelsüblicher und aktueller Sicherheitsprogramme auf seinem PC erreichen.

Außerdem sollten alle Anwender, die gerne surfen, ihre Windows-Installation zum Beispiel via LiveUpdate jederzeit auf dem neuesten Stand halten und aktuelle Browser-Versionen verwenden.

Wichtig ist dabei vor allem, die angebotenen, integrierten Sicherheitsfunktionen auch zu aktivieren. Beim Einsatz von Funkverbindungen wie WLAN ist unbedingt auf die korrekte Verschlüsselung des Datenstroms zu achten. Darüber hinaus empfiehlt sich allgemein der Einsatz einer Firewall, die als Software-Version zum Beispiel bereits in aktuellen Windows-Versionen und Hardware-Variante bereits in vielen DSL-Modems enthalten ist.

Einen gut aufbereiteten, von Herstellern unabhängigen Überblick über das Thema vermittelt das Bundesamt für Sicherheit in der Informationstechnik auf seiner Homepage unter <http://www.bsi.de/>.



Der Kugelfisch: Als Verschlüsselungsalgorithmus seit 1994 unschlagbar sicher

Sicherheits-Lexikon

SSL-Verschlüsselung:

mit 128 Bit hat diese Verschlüsselungsmethode 340.282.366.920.938.000.000.000.000.000.000.000.000 verschiedene Kombinationsmöglichkeiten. Daher kann sie von Unbefugten nicht entschlüsselt werden.

PCI Data Security Standard:

Sicherheits-Zertifikat, dessen strenge Regularien garantieren, dass Ihre Zahlungsdaten bei den teilnehmenden Online-Dienstleistern nicht in falsche Hände geraten.

Für Ihre eigene Sicherheit:

Auch Sie können aktiv zu einem sicheren Datenaustausch beitragen. Machen Sie Ihren PC Trojaner-sicher, nutzen Sie die diversen Sicherheitsfunktionen Ihres Betriebssystems und informieren Sie sich umfassend unter: <http://www.bsi.de>

Blowfish:

Der Blowfishalgorithmus ist ein symmetrischer Blockverschlüsselungsalgorithmus, der 1993 von Bruce Schneier entworfen und erstmals im April 1994 in Doctor Dobb's Journal publiziert wurde. Er wurde als „public domain“ veröffentlicht und kann frei verwendet werden. Die Schlüssellänge kann zwischen 32 Bit und 448 Bit betragen.