Internet

Risikofreies Einkaufen und Datensicherheit

Keine Angst vor dem Weihnachtsshopping auf dem Web!

Noch immer ist die Angst vor mangelnden Sicherheitsvorkehrungen eine Hemmschwelle des e-Commerce – völlig unbegründet, wenn man sich an gewisse Spielregeln hält. Auf dem Web gelten grundsätzlich dieselben Vorsichtsmassnahmen wie im normalen Leben: Ihren Bancomat-Code geben Sie ja auch nicht an Dritte weiter bzw. lassen Sie Ihre Bankkarten nicht offen herumliegen. Immerhin geben Sie öfters mal Ihre EC- oder Kreditkarte dem Personal eines Restaurants oder einer Modeboutique, mithin meist völlig unbekannten Personen, denen es ein leichtes wäre, die Karteninformationen unbeaufsichtigt abzukopieren. Machen Sie sich also mit den wichtigsten Regeln der Sicherheit beim Online-Shopping vertraut – Sie werden sehen, Einkaufen im Internet ist nicht nur einfach, sondern auch sicher.
Ich wünsche allen Leserinnen und Lesern schöne Feiertage und sage: Bis nächstes Jahr!

Thomas Vauthier
th.vauthier@bluewin.ch

Vertrauen Sie nicht blind!

Auch beim Online-Shopping gilt der gleiche Grundsatz wie im täglichen Geschäftsleben: Vergewissern Sie sich, dass der Anbieter oder Verkäufer auf dem Web vertrauenswürdig ist. Dazu gehören z.B. eine komplette Adresse mit Telefon- und eventuell Faxnummer sowie eine aktive E-Mail-Adresse. Und: Speichern Sie keinesfalls Ihre Kreditkartennummer bzw. diverse Passwörter auf Ihrem Computer. Versenden Sie keine wichtigen Daten ungeschützt via E-Mail. Es gibt viele Methoden, Ihre Daten zu knacken. Deshalb sollten finanzielle Transaktionen auf dem Web nur verschlüsselt erfolgen.

Dazu dienen Kryptografieverfahren, d.h. Techniken, die Daten so verändern oder verfremden, dass kein Unbefugter sie missbrauchen kann. Sie basieren auf Algorithmen, die Daten chiffrieren und dadurch für jeden unlesbar machen, der nicht über den passenden (Software-)Schlüssel verfügt. Ein wichtiges Mass für die Stärke (Einbruchsicherheit) eines Verschlüsselungsverfahrens ist die (in Bit gemessene) Länge des Schlüssels.

SSL – der Standard zur sicheren Datenübertragung

Seriöse Firmen setzen auf die neuen Sicherheitsstandards wie SSL. Dabei werden die Daten mit einem 128-Bit-Schlüssel chiffriert, was einer ausreichend hohen Sicherheitsstufe entspricht. Mithilfe von SSL wird der unberechtigte Zugriff auf sicherheitsrelevante Informationen wie etwa Kreditkartennummern oder persönliche Daten verhindert.

In der so genannten «Hello-Phase» baut der Kunde eine Verbindung zum Server auf und teilt mit, welche Krypto-Algorithmen (Verschlüsselungsverfahren) unterstützt werden. Der Server wählt dann auf Grund dieser Informationen ein bestimmtes Verfahren aus und teilt dies dem Client mit. Der Server sendet ein Zertifikat, das unter anderem den öffentlichen Schlüssel des Servers enthält. Das Zertifikat ist notwendig, damit der Client prüfen kann, ob die Antwort tatsächlich vom gewünschten Server stammt.

Der Client generiert einen «Session Key» für einen Datenaustausch per Private-Key-Verfahren. Diesen Schlüssel chiffriert der Client mit dem öffentlichen Schlüssel des Servers und schickt ihn an den Server. Damit können sich der Client und der Server gegenseitig authentifizieren. War das Prüfungsverfahren erfolgreich, schliessen beide Seiten (Server und Client) den initialen Verbindungsaufbau ab und chiffrieren alle weiteren Datenpakete mit dem Sitzungsschlüssel.

Tipps für geld- und nervenschonendes Online-Shopping

– Bekanntlich gibt es nicht wenige schwarze Schafe unter den Anbietern. Achten Sie auf Seriosität. Das Zertifikat oder Prüfsiegel eines renommierten Instituts bürgt in der Regel für die Vertrauenswürdigkeit eines Online-Händlers.
– Prüfen Sie bei Ihrer Bestellung zunächst die vertraglichen Rahmenbedingungen (Lieferfristen, Versandkosten). Sollten Sie im Ausland bestellen, empfiehlt es sich, den Lieferumfang vorab zu klären. Welche Garantien bietet der Händler an?
– Zahlen Sie nach Möglichkeit per Rechnung.
– Wenn Sie Ihre Kreditkartennummer weitergeben, dann nur in verschlüsselter Form. Empfehlenswert zur Verschlüsselung von Kundendaten sind das erwähnte SSL oder alternativ das Sicherheitssystem SET (Secure Electronic Transaction). Im Zweifelsfall ist es ratsam, sensible Daten entweder telefonisch oder per Fax zu übermitteln.
– Geben Sie Ihre Kreditkartendaten nur online ein, wenn die Verbindung mit SSL geschützt ist, wenn möglich mit einem 128-Bit-Schlüssel.
– Ist keine SSL-Verbindung mit 128-Bit möglich, nur die Bestellung online machen und die Kartendaten per Fax oder telefonisch an den Händler übermitteln. Im Zweifelsfall sollten Sie eine Bestellung unterlassen.
– Beantworten Sie keine Anfragen zu Ihren Kreditkartendaten, die Ihnen während eingehenden Telefonaten gestellt werden.
– Machen Sie keine Bestellungen mit der Kreditkarte von öffentlich zugänglichen Rechnern/Computern aus. Die Daten gelangen in den Zwischenspeicher und könnten vom nächsten Benutzer gelesen werden!
– Notieren Sie alle Einkäufe über SSL-Verbindungen oder erstellen Sie einen Print-Screen. Um einem «Lieferversehen» vorzubeugen: drucken Sie sich das komplette Angebot nebst Produktbeschreibung und Bestellformular aus. So können Sie, falls notwendig, die Geschäftsmodalitäten schwarz auf weiss dokumentieren.

Fortsetzung folgt ...