

Arbeitsprobe

Kategorie: IT / Telekommunikation

Kunde: rfw - Agentur für Kommunikation, Darmstadt
(für IHK, Darmstadt)

Jahr: 2004

Webshops ohne Hintertür

Sicherheit. Internet-Läden versprechen den unkomplizierten Einkauf per Maus-klick. Doch sowohl Webshop-Betreiber als auch Käufer müssen einige Sicherheitsregeln beachten, wenn der Online-Einkauf ungetrübte Freude bringen soll.

Kundenadressen, Passwörter, Kreditkartennummern und Bankdaten – die Festplatten der Internetshops bieten Datenjägern fette Beute. Deshalb muss ein Webshopbetreiber Daten gegenüber Unbefugten absichern. Firewalls sind Pflicht. Sie wirken wie virtuelle Stadtmauern. „An ihren ‚Toren‘ sorgen ‚Wächter‘ dafür, dass nur geladene Gäste Zugang finden – und ‚Hintereingänge‘ bleiben geschlossen. Um das System zuverlässig vor Hackerangriffen zu schützen, müssen auch die Webserver immer mit aktuellen Sicherheitsupdates versehen werden“, erklärt Ralf Dotzert, Leiter der Entwicklung der mtg-AG, Darmstadt. Das Software-Unternehmen ist die einzige vom Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditierte Prüfstelle in Hessen für IT-Sicherheit. „Ein zusätzlicher Virenschutz – also Polizei innerhalb der Stadtmauern – ist ebenfalls obligatorisch.“

Datenschutz gewährleisten

Datenschutz dient nicht nur der eigenen Sicherheit – die gesetzlichen Bestimmungen verpflichten den Unternehmer sogar, besondere Sorgfalt walten zu lassen. Denn Viren und ihre Verwandten dienen heute weniger dazu, Rechnersysteme zu schädigen. „Kriminelle streben eher danach, Schadprogramme möglichst lange und unbemerkt in fremden Netzen zu verstecken. So manche Unternehmensfest-

platte diene im Hintergrund schon als Datenlieferant für Betrüger“, sagt Andrea Klenk, Leiterin Security Solutions bei mtg.

Datenverkehr verschlüsseln

„Kein Mensch käme auf die Idee, die Daten seiner Kreditkarte per Postkarte an einen Versandhändler zu schicken“, sagt Ralf Dotzert. „Hacker können den Datenverkehr im Internet jedoch einfach mitlesen. Deshalb müssen persönliche Daten auf dem Weg zwischen Kunden und Webshop verschlüsselt werden – sozusagen als virtueller Einschreibebrief.“ Die Techniken hierzu sind ausgereift und sicher.

Der Käufer erkennt aktive Verschlüsselung an gelb unterlegter Seitenadresse im Browser oder einem kleinen geschlossenen Schloss in der Statusleiste des Programms. „Wer sich unsicher ist, sollte nicht zögern, den Shopbetreiber anzurufen und nachzufragen.“ Unbekannte oder unverständliche Meldungen während der Sitzung sind ebenfalls Warnsignale. „Tauchen sie auf, ist es am besten, das Shopprogramm zu schließen und ebenfalls zum Telefontaster zu greifen“. so Dozert.

Sichere Passwörter verwenden

Online-Schnäppchenjäger können die Sicherheit beim virtuellen Einkauf selbst erhöhen. Damit ein Hacker oder spezielle Suchprogramme ein Passwort nicht „erraten“ können, empfiehlt Andrea Klenk möglichst lange und auf den ersten Blick sinnlose Zeichenfolgen. Hier helfen Eselsbrücken: Beispielsweise merkt sich der Nutzer einen ganzen Satz und setzt das Passwort aus den Anfangsbuchstaben zusammen. „Freitags isst die Oma immer dreimal Fisch mit Soße“ wird dann zu ‚FidOi3FmS‘ – darauf muss ein Datenräuber erst mal kommen.“