Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Fachhochschule Gelsenkirchen

Mitglied im:

Netzwerk Elektronischer Geschäftsverkehr

Sicherheitstipps für den eigenen Onlineshop

Einen eigenen Onlineshop zu erstellen ist heute durch individualisierbare Standarddesigns bereits mit wenigen Klicks und zu relativ geringen Kosten möglich. Doch wer Produkte und Dienstleistungen im Internet anbietet, hat seinen Kunden gegenüber auch einige Pflichten zu beachten. Die Konkurrenz ist groß. Neben einem günstigen Preis ist vor allem die Sicherheit ein wichtiges Kriterium bei der Kaufentscheidung. Wer seinen Kunden größtmögliche Sicherheit bietet, profitiert langfristig selbst davon. Was genau Sie zu beachten haben, erfahren Sie in diesem Sicherheitstipp.

Achten Sie bei Ihrem Onlineshop auf einen angemessenen Basisschutz!

Der Server des Onlineshops muss vor einer Vielzahl von Bedrohungen, wie Schadsoftware und Hackern, geschützt werden. Installieren Sie deshalb eine Firewall, die nur den tatsächlich benötigten Diensten eine Kommunikation von außen (z.B. http, https und ssh) bzw. nach außen (z.B. http und https für das Empfangen von Sicherheitsupdates) erlaubt. Halten Sie das Betriebssystem und sämtliche installierten Dienste zum Schutz vor Sicherheitslücken immer auf dem neuesten Stand. Konfigurieren Sie den Server so, dass Programme nur mit der nötigen Berechtigung ausgeführt werden können und von Kunden hochgeladene Dateien nur beschränkte Rechte besitzen. Erstellen Sie mindestens einmal täglich eine Datensicherung, für den Fall eines Verlusts durch Diebstahl oder Festplattenschaden. Sichern Sie Ihre Daten physikalisch an einem anderen Ort als sich Ihre Originaldaten befinden.

Lassen Sie nur sichere Passwörter zu!

Geben Sie Ihren Kunden feste Regeln für die Vergabe eines sicheren Passworts vor. Ein sicheres Passwort besteht aus mindestens 10 Zeichen, darunter Groß- und Kleinbuchstaben, Nummern und Sonderzeichen. Es entbehrt jeder Logik und ist ein keinem Lexikon zu finden (ausführliche Informationen dazu, finden Sie in dem vom Netzwerk Elektronischer Geschäftsverkehr bereits erschienenden IT-Sicherheitstipp „Wie erstelle ich ein sicheres Passwort?“). Um Ihren Kunden größtmögliche Sicherheit zu bieten, sollte jeder fehlgeschlagene Login-Versuch protokolliert und beim nächsten Login angezeigt werden. So ist schnell ersichtlich, ob ein Unbefugter versucht hat sich Zugang zu verschaffen. Wird eine zuvor definierte Anzahl von Fehlversuchen überschritten, sollte der Nutzeraccount automatisch gesperrt und der Kunde via E-Mail automatisch informiert werden.

Nutzen Sie eine Verschlüsselung beim Austausch von Kundendaten!

Die Adresse des Kunden, seine Bankverbindung und sein Kaufverhalten sind bares Geld wert. Deshalb nehmen Kriminelle für den Diebstahl von Datensätzen auch größeren Aufwand in Kauf. Um Datenmissbrauch vorzubeugen, sollten Sie sensible Daten ausschließlich verschlüsselt übertragen. Eine Verschlüsselung über das im Internet etablierte Verschlüsselungsprotokoll TLS (besser bekannt als SSL) erkennt man zum einen am Schloss-Symbol in der unteren Browserleiste. Zum anderen beginnt die Internetadresse verschlüsselter Webseiten mit „https“ statt wie gewöhnlich mit „http“. Um SSL anbieten zu können, müssen Sie ein zeitlich befristetes Zertifikat erwerben.

Bieten Sie sichere Zahlverfahren an!

Je mehr Bezahlverfahren, desto höher die Kaufwahrscheinlichkeit. Die Zahlung per Kreditkarte und Bankeinzug sind die aktuell gängigsten Formen. Hierfür muss der Kunde bei jeder Bestellung seine Kreditkarten- bzw. Bankdaten über das Internet an Sie übermitteln. Bezahlsysteme wie „PayPal“ und „Click & Buy” gelten als sicher und sind für den Kunden äußerst bequem. Die sensiblen Bankdaten müssen nur einmalig übertragen werden. Die Zahlung per Nachname gilt für den Kunden zwar auch als relativ sicher, bringt jedoch auch eine zusätzliche Zustellgebühr mit sich.

Lassen Sie Ihren Onlineshop zertifizieren!

Machen Sie doch Sicherheit zu Ihrem Merkmal. Prüfstellen wie „Trusted Shops“, „EHI“ oder der TÜV erteilen nach eingängigem Test die Bestätigung, dass der Online-Shop hinsichtlich Preistransparenz, Lieferbedingungen, Datenschutz und rund 100 weitere Kriterien als vertrauenswürdig einzustufen ist. Sicherheitslücken, die eventuell übersehen worden sind, lassen sich so auch effizienter aufspüren und beheben. Auch die Angabe eines konkreten Ansprechpartners für Fragen zur Sicherheit und des Datenschutzes erweckt bei Ihren Kunden einen seriösen Eindruck.

Kennen Sie Ihre gesetzlichen Pflichten!

Wer fahrlässig mit Kundendaten umgeht, riskiert nicht nur einen erheblichen Imageschaden, sondern auch empfindliche Geldbußen und sogar Gefängnisstrafen. Betreiber von Onlineshops sollten sich deshalb ausführlich mit dem Bundesdatenschutzgesetz und dem Telemediengesetz auseinandersetzen. Generell gilt: Erlaubt ist nur die Speicherung von Daten, die unbedingt zur Abwicklung des Kaufvorganges notwendig sind. Die Verwendung von Kundendaten für Marketing-Maßnahmen ist nur nach vorheriger ausdrücklicher Genehmigung (zum Beispiel durch das Setzen eines Häkchens im Bestellformular) erlaubt. Speichern Sie Ihre Kundendaten auf einem Computer, der nicht an das Internet angeschlossen ist. So laufen Sie nicht Gefahr, die Daten durch einen Hackerangriff an Unbefugte zu verlieren. Machen Sie außerdem für den möglichen Ausfall des Systems regelmäßige Sicherungskopien Ihres Kundenbestandes auf zusätzlichen Speichermedien.

Autoren:
Dipl.-Inform.(FH) Sebastian Spooren
Dustin Pawlitzek
Prof. Dr. (TU NN) Norbert Pohlmann

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit – if(is)

Weiterführende Informationen:
http://www.ec-net.de
http://www.internet-sicherheit.de
https://www.it-sicherheit.de
http://www.bsi.bund.de

Bildquelle: Falko Matte - Fotolia.com

Das Netzwerk Elektronischer Geschäftsverkehr
Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk" etabliert. Das Netzwerk ist das einzige bundesweite Angebot seiner Art und verzeichnet jährlich rund 30.000 Besucher in Beratungen und Veranstaltungen. Es stellt Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)
Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de

Sichere E-Geschäftsprozesse in KMU und Handwerk
Der IT-Sicherheitstipp wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk" des Netzwerks Elektronischer Geschäfts verkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.ec-net.de/sicherheit