published as: Torsten Becker, Christoph Meinel: Sicherheit: Der entscheidende Erfolgsfaktor für E-Commerce und M-Commerce; ONLINE 2003 Düsseldorf (Germany), 2003, pp. C421.03-C421.08.

Sicherheit: Der entscheidende Erfolgsfaktor für E-Commerce und M-Commerce*

Torsten Becker, Christoph Meinel
FG Institut für Telematik, Universität Trier
54286 Trier
www.telematik-institut.org
{becker, meinel}@ti.uni-trier.de

1 Einleitung

Laut „(N)ONLINER Atlas 2003“[1] sind über 50 Prozent der Deutschen im Jahr 2003 im Internet. Dies ist im Vergleich zum Vorjahr eine Steigerung um 8%. Auch der Anteil der Online-Käufer nimmt kontinuierlich zu. Mittlerweile haben unter den Online-Nutzern rund zwei Drittel Erfahrungen mit Online-Käufen und -Buchungen. Das heißt aber auch, dass etwa ein Drittel der Online-Nutzer keine Geschäfte über das Internet abwickeln. Laut einer Studie der Unternehmensberatung Accenture[2] liegt beispielsweise die größte Hemmschwelle der Kunden bei einem Online-Kauf darin, persönliche Daten ungeschützt über das Internet zu übermitteln. Dies führt laut Accenture in Deutschland zu einem jährlichen Umsatzausfall in Milliardenhöhe. Auch Fittkau und Maaß haben in einer Studie ermittelt, dass bei den Anforderungen der Nutzer an Online-Finanzdienstleister die Sicherheit der Datenübertragung im Vordergrund steht[3]. Eine Studie von ComCult Research verstärkt dies: „Sicherheitsbedenken der Nutzer sind die größte Barriere beim Online-Shopping. Sie werden als Hauptgrund dafür genannt, dass Nicht-Shopper bisher noch keine Erfahrung im Online-Shopping gesammelt haben und das Shopper nicht häufiger online bestellen. Shopper und Nicht-Shopper sind sich einig, dass die sichere Übermittlung der Zahlungsdaten bedenklich ist.“[4] Zu den Erfolgsfaktoren im E-

---

** in Proc. ONLINE'03 (Düsseldorf), Congress IV: e/mSecurity, C421.01-C421.08*

1 *Der „(N)ONLINER Atlas 2003“ ist eine gemeinsame Untersuchung von TNS Emnid und der Initiative D21 (www.nonliner-atlas.de)*

2 *„IT Security - Wachstumsfaktor im E-Business“ (www.accenture.de)*

3 *W3B-Report „Banking & Broking im Internet“, Fittkau & Maaß 2002, www.fittkaumaass.de*

4 *Studie E-Commerce Facts 2.0 von ComCult Research (www.comcult.de)*

Commerce und M-Commerce gehören demnach der konsequente Aufbau von Vertrauen, die Einhaltung von Datenschutzanforderungen und die sichere Datenübermittlung.

2 E-Commerce und M-Commerce

Unter E-Commerce versteht man die elektronische Abwicklung von Geschäftsprozessen zwischen zwei oder mehreren Parteien unter Zuhilfenahme von Informations- und Kommunikationstechnologien. E-Commerce kann sowohl zwischen Unternehmen („Business to Business“ - B2B) als auch zwischen Unternehmen und ihren Kunden („Business to Consumer“ - B2C) stattfinden. Daneben gibt es noch weitere Formen des E-Commerce, wie z.B. zwischen Privatpersonen („Consumer to Consumer“ - C2C) oder die Einbeziehung der öffentlichen Verwaltung („E-Government“). Die Geschäftsprozesse können sowohl über offene Netze (z.B. Internet) als auch über private Netze (z.B. Intranet, VPN) abgewickelt werden.

E-Commerce bezeichnet nicht nur den elektronischen Handel mit Waren und Dienstleistungen, sondern vielmehr den gesamten elektronischen Geschäftsverkehr, also zum Beispiel auch Finanztransaktionen.

M-Commerce kann als ein Teilgebiet des E-Commerce aufgefasst werden, wobei die Geschäftsprozesse mit Hilfe von mobilen Kommunikationstechnologien abgewickelt werden. Mit mobilen Endgeräten lassen sich nicht nur weitere Kommunikations- und Absatzkanäle erschließen, sondern sie bieten auch eine neue Dimension in der individuellen Kundenansprache (z.B. sogenannte „Location Based Services“). Aufgrund der weiten Verbreitung von mobilen Geräten, besteht ein großes Potential für M-Commerce-Anwendungen. Trotz vielversprechenden Prognosen[5], sind die Umsätze im Bereich M-Commerce aber noch nicht bedeutend.

---

5 *Das Marktforschungsinstitut Durlacher Research (www.durlacher.com) prognostizierte im November 1999 für das Jahr 2003 im Bereich M-Commerce ein europäisches Marktvolumen in Höhe von 23,6 Billionen Euro.*

3 Erfolgsfaktor Sicherheit

Eine Reihe von Faktoren sind verantwortlich für den Erfolg einer E-Commerce-Anwendung. Oftmals nicht beachtet, aber aus unserer Sicht entscheidender Erfolgsfaktor ist die Sicherheit.

3.1 Sicherheitsbedürfnisse

Bei jeder E-Commerce-Anwendung bestehen Sicherheitsbedürfnisse, die mehr oder minder erfüllt sein müssen, damit es überhaupt zu einer Tranksaktion kommt.

In erster Linie muss natürlich die Verfügbarkeit der Funktionen eines Systems und seiner Informationen gewährleistet sein. Darüber hinaus muss bei vielen Tranksaktionen die Vertraulichkeit garantiert sein. Nur befugte Personen dürfen in Kenntnis der übermittelten Informationen gelangen. Ferner muss die Integrität der übermittelten Daten sowie die Nichtabstreitbarkeit einer Transaktion sichergestellt sein. Zudem muss die Authentizität der Kommunikationspartner immer gewährleistet sein.

Die Erfüllung dieser Bedürfnisse ist zum Teil auch gesetzlich vorgeschrieben. So ist beispielsweise die Gewährleistung der Vertraulichkeit personenbezogener Daten auch eine Anforderung des Datenschutzes.

Die Sicherheitsbedürfnisse werden deutlich, wenn man eine Übermittlung von Kreditkartendaten über das Internet als Beispiel betrachtet. Bei solch einer Transaktion sollte gewährleistet sein, dass

- die Daten den Empfänger erreichen (Verfügbarkeit),
- die Daten nur vom Sender und Empfänger gelesen werden können (Vertraulichkeit)
- die Daten während der Übertragung nicht verändert werden (Integrität),
- der Empfänger sicher sein kann, dass die Daten vom angegebenen Absender stammt (Nichtabstreitbarkeit) und
- der Empfänger sicher sein kann, dass der Sender auch wirklich der Eigentümer der Kreditkarte ist (Authentizität).

3.2 Hemmnisse des E-Commerce aufgrund fehlender Sicherheit

Ist ein Sicherheitsbedürfnis eines Beteiligten nicht oder nur unzureichend erfüllt, so wird in der Regel eine Transaktion nicht zustande kommen. Fehlende oder unzureichende Verschlüsselung ist ein häufiger Grund für den Abbruch einer Transaktion, da die Vertraulichkeit der Daten in diesem Fall nicht gegeben ist.

Darüber hinaus können beispielsweise beweiserhebliche Vorgänge nicht oder nur eingeschränkt elektronisch durchgeführt werden, da technische Komponenten für die Abwicklung dieser mindestens auf einer Seite der Geschäftspartner fehlen, z.B. für eine qualifizierte elektronische Signatur. Mit einer qualifizierten elektronischen Signatur kann der Urheber und die Integrität von Daten zuverlässig festgestellt werden. Somit erlangt die elektronische Signatur als Substitut zur handschriftlichen Unterschrift eine entsprechende Rechtswirkung[6].

Da die Authentizität eines Kunden (insbesondere bei einem Neu-Kunden) bei einer Transaktion über offene Netze (Internet) nicht ohne weiteres gewährleistet werden kann, liefern viele Online-Shops ausschließlich per Vorkasse oder per Nachnahme. Diese Einschränkung schreckt viele Interessenten ab.

Häufig werden bei Webseiten erweiterte Browser-Funktionen wie JavaScript, Java, ActiveX und Cookies genutzt. Der Browser des Geschäftspartners muss diese zulassen, damit es überhaupt zu einer Transaktion kommen kann. Da aber viele Sicherheitslücken auf diesen Browser-Funktionen beruhen, haben einige sicherheitsbewusste Anwender diese Optionen deaktiviert. Obwohl dieser Faktor zurzeit wirtschaftlich nur marginal den Erfolg eines Unternehmens beeinflusst, sollte diesem Aspekt lang- und mittelfristig Beachtung geschenkt werden.

Speziell im Bereich des M-Commerce gibt es noch einige Sicherheitsprobleme. So wurde beispielsweise die Verbreitung der WLAN-Technologie nach Bekanntwerden von Schwachstellen bei den verbreiteten Authentisierungsmechanismen und Verschlüsselungsverfahren für WLANs gehemmt.

3.3 Schäden aufgrund fehlender Sicherheit

Neben den Schäden durch abgebrochene bzw. nicht stattgefundene Geschäfte aufgrund von nicht erfüllten Sicherheitsbedürfnissen, führen aufgetretene

---

6 Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Stand 22. Mai 2001

Sicherheitsmängel bei einer Anwendung oder einem System zu einem finanziellen Schaden. Nicht nur das Ausnutzen einer Schwachstelle durch einen oder gar mehrere Betrüger, sondern auch der Reputationsverlust durch Bekanntwerden dieses Sicherheitsproblems führt zu einem Schaden. Dabei verursacht der Imageverlust in der Regel einen wesentlich höheren finanziellen Schaden, als der Betrugsfall an sich. Deshalb ist es in vielen Fällen für ein Unternehmen besser, den durch einen Betrug entstandenen Schaden hinzunehmen, als beispielsweise eine Anzeige gegen den Betrüger zu erstatten, wodurch der Betrug publik gemacht wird.

Des Weiteren kann ein Ausfall der gesamten oder eines Teils der IT-Infrastruktur zu einem erheblichen finanziellen Schaden eines Unternehmens führen. Diese Ausfälle können beispielsweise durch Sabotage, Viren, „Denial-of-Service“-Attacken aber auch durch defekte Hard- oder Software verursacht werden. Dies kann die Existenz eines Unternehmens bedrohen, wenn nicht frühzeitig geeignete Schutzmaßnahmen ergriffen worden sind.

4 Konsequenzen

Vielen Unternehmen ist der erhebliche Einfluss der Sicherheit auf ihren Unternehmenserfolg nicht bewusst. Gerade in Unternehmen, die sich auf E-Commerce spezialisiert haben, führt dies in den meisten Fällen früher oder später zur Erfolglosigkeit des Unternehmens.

Um dem entgegenzuwirken, muss der IT-Sicherheit in einem Unternehmen ein hoher Stellenwert eingeräumt werden. Technisch sind benutzerfreundliche Systeme und Verfahren, um einen sicheren und erfolgreichen E-Commerce zu gewährleisten, vorhanden. Dabei ist zu beachten, dass Sicherheit kein Zustand, sondern ein Prozess ist. Laufende Überprüfungen und Verbesserungen sind unverzichtbar. Es empfiehlt sich hier ein Sicherheitsmanagement aufzubauen, das die Informationssicherheit planmäßig herstellen und überwachen soll, damit reale und daraus resultierende wirtschaftliche Schäden im Unternehmen verhindert werden können.

Ist die Sicherheit der E-Commerce-Anwendungen eines Unternehmens sichergestellt, so kann dies als Werbebotschaft eingesetzt werden. Durch Überprüfung und Bestätigung (Zertifizierung) der Sicherheit durch einen neutralen Dritten, kann zudem das Vertrauen und somit die Akzeptanz von Online-Verbrauchern verstärkt und somit ein entscheidender Wettbewerbsvorteil gegenüber Konkurrenten mit einem niedrigen Sicherheitsniveau erzielt werden.

Durch Einführung von Sicherheitstechniken ergeben sich zudem neue Potentiale für einen Anbieter im E-Commerce. Viele Anwendungen, bei denen beispielsweise die gesicherte Authentizität der Beteiligten oder die Vertraulichkeit der Daten entscheidende Bedeutung haben, sind nur bei Gewährleistung eines hohen Sicherheitsniveaus möglich.

Da die Sicherheit und damit der Erfolg des E-Commerce auch von der Sicherheit auf Client-Seite abhängt, sollte ein Interesse an einer Verbreitung entsprechender Sicherheitstechniken bestehen; insbesondere seitens der öffentlichen Hand mit ihren E-Government-Bestrebungen[7]. Die Einführung einer Bürgerkarte als digitaler Ausweis mit Signaturfunktion wäre ein geeignetes und dringend benötigtes Mittel, um flächendeckend beweiserhebliche Vorgänge im E-Commerce elektronisch durchführen zu können. Somit wäre eine essentielle technische Voraussetzung zur Sicherstellung der Vertraulichkeit, der Integrität, der Authentizität und der Nichtabstreitbarkeit gegeben.

Während bei der Entwicklung des Internets Sicherheitserwägungen zunächst nicht bedacht wurden, besteht speziell im M-Commerce noch die Chance, bei der Einführung neuer Techniken und Standards Sicherheitsaspekte zu beachten, damit Sicherheitsverfahren bei den mobilen Kommunikationstechnologien mit weitaus geringerer Verzögerung entwickelt und eingeführt werden als im Internet.

---

7 E-Government-Initiative der Bundesregierung (www.bundonline2005.de)