

# Kein Geschäft ohne Vertrauen

**Fehlende Nähe als psychologische Barriere und Unsicherheiten bezüglich Rechtsverbindlichkeit und Datenschutz hemmen noch den großen Durchbruch des e-Shoppings. Was kann IT Security zum notwendigen Vertrauensaufbau beitragen?**

Vertrauen und Verbindlichkeit sind im e-Commerce kritische Erfolgsfaktoren. Ein Kunde muss sich sicher sein, dass mit seinen Daten vertraulich umgegangen wird, ein Missbrauch durch Dritte weitestgehend ausgeschlossen ist und seine Online-Transaktionen verbindlich abgewickelt werden, und dass er schließlich die gewünschte Ware oder Dienstleistung erhält. Nicht zuletzt muss auch der Anbieter sein berechtigtes Interesse an der Verbindlichkeit von Aufträgen abgesichert wissen.

Zahlreiche Studien zeigen, dass mangelndes Vertrauen die Hauptursache für den Verzicht auf Online-Einkäufe ist. Auswertungen von Website-Statistiken belegen, dass rund 60% aller begonnenen Online-Geschäfte abgebrochen werden, wenn der potenzielle Kunde persönliche Daten eingeben soll. Bedenklich stimmen die Ergebnisse einer Untersuchung zu Vertraulichkeit und Informationspolitik der deutschen TÜV Nord Security. Von mehr als 100 Online-Shops verfügen 90% über unzureichendes Datenschutzverständnis und gar «... nur 5 Prozent der untersuchten Netze (waren) ohne Mängel, so dass Hacker und Cracker quasi freien Zutritt zu einer Vielzahl der Shops haben.»

## Vertrauen aufbauen

Beim Aufbau eines geeigneten Handlungsrahmens für einen sicheren und verbindlichen elektronischen Geschäftsverkehr spielt die IT Security eine wichtige Rolle. Genauer gesagt eine Doppelrolle, denn sie stellt nicht nur sichere

Infrastrukturen und effiziente Verfahren zur Abwicklung elektronischer Geschäftsvorfälle bereit, sondern liefert auch die erforderlichen Revisionsmethoden im Rahmen des IT Audit.

Um als e-Business Enabler zu gelten, muss Sicherheitsarchitektur nicht nur die Implementierung von Sicherheitstechnik, sondern den gesamten Bereich

«Vertrauen und Verbindlichkeit sind im e-Commerce erfolgskritisch.»

der Online-Geschäftsprozesse, über Software-Systeme, Plattform, Kommunikation und Datenhaltung bis hin zur Partneranbindung, beinhalten.

## Sichere Infrastruktur als Basis

Um Vertrauen in die Sicherheit offener Netze wie das Internet zu schaffen, ist eine Infrastruktur erforderlich, die folgende Grundwerte sichert:

- Integrität: Die Daten erreichen den Empfänger unverändert.
- Authentizität: Die Daten stammen wirklich vom Absender, für den er sich ausgibt.
- Vertraulichkeit: Die Daten kann nur der vorgesehene Empfänger lesen.
- Zurechenbarkeit: Das Absenden bzw. Empfangen von Daten kann nicht abgestritten werden.

Die Grundlagen für ein risikogerechtes Sicherheitsmanagement sind der Einsatz moderner kryptographischer Verfahren, die Vertraulichkeit gewährleisten, und digitaler Signaturen, die zur Identifizierung der Kommunikationsteilnehmer (ist

mein Kommunikationspartner derjenige, für den er sich ausgibt?) und zur Authentifizierung von digitalen Dokumenten (erreicht mich die Information unverfälscht und unverändert?) dienen.

### Zertifikate schaffen Authentizität und Verbindlichkeit

Digitale Signaturen machen die Urheberschaft von Daten nachprüfbar und garantieren deren Unverfälschtheit, da Informationen aus den Daten in die Erzeugung der digitalen Signatur einfließen. Die Verfahren der digitalen Signatur basieren auf dem Public-Key-Verschlüsselungsverfahren, bei dem jeder Teilnehmer ein Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel besitzt. Was mit dem privaten Schlüssel verschlüsselt wird, kann nur mit dem öffentlichen entschlüsselt werden und umgekehrt. Diese Eigenschaft wird sowohl für die Verschlüsselung (Vertraulichkeit der Nachricht) wie auch für die elektronische Signatur (Authentizität der Nachricht) eingesetzt.

Zur effektiven Nutzung bedient man sich einer Public Key Infrastruktur PKI, um jederzeit Authentizität und Gültigkeit des öffentlichen Schlüssels eines jeden Teilnehmers der Infrastruktur eindeutig zu ermitteln. Die Infrastruktur beruht auf dem gemeinsamen Vertrauen der Nutzer in eine zentrale Instanz, die als Zertifizierungsagentur die Authentizität der Schlüssel bestätigt.

Der elektronischen Signatur kommt somit die Funktion einer eigenhändigen Unterschrift zu, mit dem Unterschied, dass sie zusätzlich vor Verfälschung des Dokuments schützt. Diverse Rechtsverordnungen zur digitalen Signatur begründen damit die Rechtsverbindlichkeit elektronischer Verträge. Innerhalb der EU existiert dazu eine Richtlinie, die bis Juni 2001 in nationales Recht umzusetzen ist. Auch die Schweiz hat am

1. Mai 2000 ein Gesetz zur digitalen Signatur verabschiedet. Noch sind diese Rechtsverordnungen nicht harmonisiert und auch die in der EU-Richtlinie vorgesehenen Vereinbarungen zur gegenseitigen Anerkennung von Signaturen mit Drittstaaten lassen auf sich warten.

Um Zertifikate auf breiter Basis einzusetzen, müssen sie wie ein Personalausweis oder eine Identity Card eindeutig mit dem Inhaber verbunden sein, und alle Anbieter müssen diese «Card» akzeptieren, unabhängig von welcher Zertifikatsagentur es stammt.

### Geprüfte Qualität

Trust-Modelle oder Prüfsiegel basieren auf der Idee, dass beim Kunden über die Vergabeanforderungen Vertrauen in die Zuverlässigkeit des Shops und die Vertraulichkeit im Umgang mit seinen persönlichen Daten erzeugt wird. Ein erster Ansatz kam aus den USA. Das Zertifikat der CPA WebTrust in den USA bewertete folgende Kriterien:

- Sicherheit der Site
- Vertraulichkeit der Kundendaten
- Verbindlichkeit der elektronisch vereinbarten Geschäfte
- Einrichtung eines Beschwerde-Managements
- regelmässige Revision der Site

Analog dazu wurden in Deutschland verschiedene Prüfsiegel entwickelt, die zur Zeit teilweise auf den europäischen Raum ausgeweitet werden. Ihr Vorteil liegt eindeutig darin, dass sie weniger

komplex und daher rasch zu realisieren sind.

### Security Policy als Gestaltungsaufgabe

Im Rahmen eines jeden Online-Angebotes sollten Nutzer vorab über die in einer Security Policy festgelegten Be-

«Für breite Einsetzbarkeit brauchen digitale Signaturen den Status eine Identity Card.»

dingungen für den Umgang mit personenbezogenen Daten informiert werden. Je nach Geschäftsvorfall muss der Anwender diese sogar bewusst anerkennen. Schwierig dabei ist, den Benutzer mit geringem Bedienungsaufwand durch die Regeln der Policy zu führen, ihm andererseits die Möglichkeit zu erschweren, die Policy ungelesen wegzuklicken. Im Wesentlichen umfasst eine Policy die Art der Benutzer-Identifizierung, die Geschäftsprozesse, das Schlüsselmanagement und die Sicherheitsmaßnahmen. Sicherheit betrifft nicht nur Durchsetzungsfähigkeit von Recht sondern auch



die Fragen des Schutzes personenbezogener Daten und damit den Schutz vor unerwünschten Marketingaktivitäten.

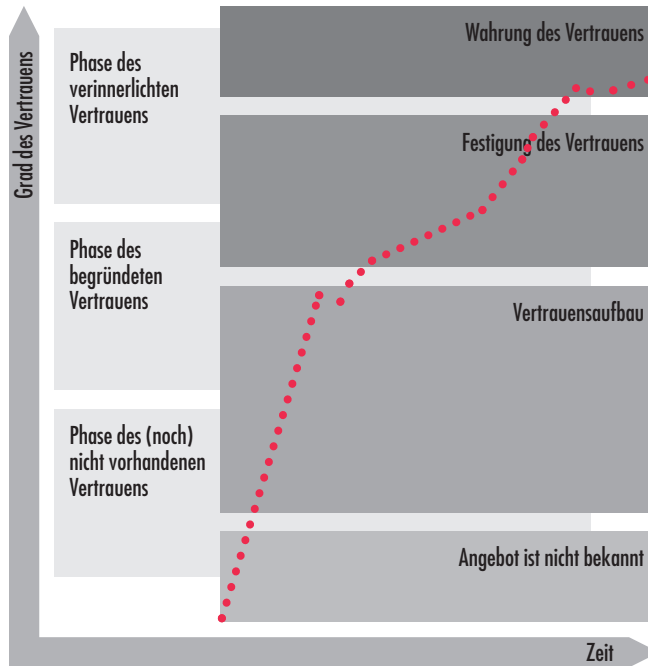
«Geprüfte Sicherheit: Ein Siegel schafft Vertrauen.»

Viele Websites melken interessierte Besucher datenmäßig ab. Fragebögen sind auszufüllen, über Cookies werden Informationen gesammelt, Online-Profile für Werbung genutzt. Wenn die kritische

Akzeptanzschwelle überschritten ist, können aus den Segnungen des 1:1-Marketings rasch elektronische Rohrkrepiere werden. Datenschutz konsequent auch in den Online-Geschäftsbereichen zu verankern, ist insofern keine lästige Pflicht, sondern geschäftserhaltende Notwendigkeit. Eine Privacy Policy soll den verantwortungsvollen Umgang mit Nutzerdaten sicherstellen und damit das Vertrauen der Nutzer stärken.

### Elektronische Verträge etablieren sich

Die für das B2C-Geschäft (Business-to-Consumer) formulierten Bedingungen gelten in gleichem Maße für den Bereich Business-to-Business (B2B) und den relativ neuen Collaborative Commerce. Der c-Commerce ist eine Erweiterung des B2B, wobei derzeit der wesentliche Unterschied des B2B zum Privatkunden-Bereich darin liegt, dass die Geschäftspartner auf konventionellem Wege vorab Kooperationsverträge abschließen, die das gemeinsame Ge-



Quelle: Cheskin Research und Studio Archetype/Sapient: eCommerce Trust Study, 1990

schäft auf klare rechtliche Grundlagen stellen.

Betrachtet man neuere Initiativen wie beispielweise «ebXML», ein XML-Framework zur Unterstützung firmenübergreifender e-Commerce-Prozesse, das von der UN/CEFACT (United Nations Centre for Trade Facilitation) betrieben wird und als Pendant zum bekannten Standard EDIFACT gesehen werden kann, und UDDI (Universal Description, Discovery and Integration), eine Initiative für einen Online-Service zur Publikation, Suche und Integration von e-Services, die dann auch online bestellbar sein sollen, dann wird auch in diesem Bereich der elektronische Vertrag den konventionellen zumindest teilweise verdrängen.

Alle diese Ansätze sind noch relativ neu und nicht konsolidiert. Noch im laufenden Jahr soll ebXML in einer ersten einsetzbaren Version verabschiedet werden. Ähnliches gilt für «RosettaNet», das soeben in der Version 1.0 freigegeben wurde. «BizTalk» gewinnt

unter anderem durch die Einführung des neuen Übertragungsprotokolls SOAP (Simple Object Access Protocol) zu zusätzlichen Entwicklungsschub.

### Gleichrangige Ziele

Aktuelle e-Commerce-Angebote müssen sichere Plattformen und zuverlässige Prozesse für die Abwicklung von Geschäften ohne Zertifikate bereitstellen und gleichzeitig für die Verwendung zertifikatsbasierter Prozesse offen sein. Um dies zu gewährleisten, benötigt man durchgängige und evolutionsfähige Sicherheitskonzepte, die einen schnellen

«IT Security muss den Balanceakt zwischen risikogerechtem Sicherheitsniveau und zukunftsfähiger Offenheit schaffen.»

Einstieg in den e-Commerce erlauben und dafür die notwendigen Rahmenbedingungen im Sinne von Vertrauen und Verbindlichkeit liefern.

Ergänzend ist ein international verfügbares Netz von gegenseitig anerkannten Zertifikatsagenturen unabdingbar, wie

es derzeit im Bankenbereich mit IDEN-TRUS aufgebaut wird. Die grossen e-Commerce-Anbieter, die Betreiber von Marketplaces und die seit langem am Markt agierenden Versandhäuser hätten das Potenzial vereinheitlichte PKI-Systeme aufzubauen. Leider gehen gerade letztere heute eher den Weg der eigenen Kundenkarten, was kurzfristig die Kundenbindung erhöht, mit der Kartenflut aber den e-Commerce insgesamt hemmt. Alternativen dazu sind Loyalty-Konzepte, wie beispielsweise das sehr erfolgreich eingeführte «Payback» in Deutschland. Beste Voraussetzungen wären geschaffen, wenn sich Banken und Nicht-Banken zur gemeinsamen Nutzung des IDEN-TRUS-Netzes entschließen könnten.

### **Aus einer Hand**

Systor bietet mit den IT Security Services das Know-How und die Erfahrung für den Aufbau sicherer Infrastrukturen, und mit den IT Audit Services die erforderliche Erfahrung im Bereich von IT-Revisionen, um vertrauenswürdige e-Commerce-Sites aufzubauen. Gleichzeitig stehen vielfältige Erfahrungen im Bereich der Prozess-, Applikations- und B2B/B2C-Integration zur Verfügung, um Anbieter bei der Implementierung durchgängiger e-Commerce-Prozesse zu unterstützen und so den erfolgskritischen Vertrauensaufbau zu fördern.

## **Wie Vertrauen entsteht**

Aus einer Studie von Cheskin Research und Studio Archetype/Sapient lassen sich folgende Ergebnisse zusammenfassen: Erscheinungsbild und Nutzerführung sind erste wesentliche vertrauensbildende Faktoren beim Kennenlernen eines Angebots. Aus Sicht der IT Security ist die Phase des «begründeten Vertrauens» entscheidend. Dann sucht der Kunde nach Kriterien, die ein Vertrauen in das Angebot rechtfertigen: Erklärungen zum Umgang mit vertraulichen Daten, Angaben über die Art der Einbindung von Logistik- oder Payment-Partnern, Medienberichte über Testkäufe und deren Abwicklung, und nicht zuletzt der Bekanntheitsgrad des Anbieters in der e-Welt oder gegebenenfalls der Old Economy. Vertrauensfördernd wirken eine klare und verständliche Kommunikation der Sicherheitspolitik des Anbieters, die Verwendung anerkannter Verschlüsselungsverfahren für die Datenübertragung, wie beispielsweise SSL mit 128 Bit oder unabhängige Prüfsiegel. Wenn der Kunde erste erfolgreiche und für ihn zufriedenstellende Testkäufe getätigt hat, beginnt die Phase des «verinnerlichten Vertrauens». Das heisst, er setzt voraus, dass er dem Anbieter vertrauen kann. Die Tatsache, dass er nach einer ersten Transaktion nicht plötzlich mit unaufgefordert zugesandten Werbe-e-Mails auch anderer Anbieter überhäuft wird, ist auch ein solches Kriterium.

»» Eine Liste mit den wichtigsten Links sowie weitere Informationen zu diesem Artikel erhalten Sie von [ulrich.moser@systor.com](mailto:ulrich.moser@systor.com), Telefon +41 1 405 35 56.