Technologien und Strategien zum Aufbau von Vertrauen im Electronic Commerce[1]

Mary Anne Patton and Audun Jøsang
Distributed Systems Technology Centre[2],
Brisbane, Australia

Abstract:

Mangelndes Konsumentenvertrauen in eCommerce-Betreiber, eCommerce-Technologien und die sozialen, finanziellen und rechtlichen Rahmenbedingungen von eCommerce stellen wesentliche Hindernisse für die umfassende Akzeptanz von business-to-consumer eCommerce dar. Die meisten der aus der physischen Welt gewohnten Signalsysteme zur Bewertung von Vertrauenswürdigkeit sind online nicht verfügbar. Dieser Artikel gibt einen Überblick über einige der Arbeiten, die sich mit der Entwicklung alternativer Methoden zur Bewertung, Kommunikation und Etablierung von Vertrauen in diesem Kontext befassen. Die angeführten Beispiele sind einer Vielzahl wissenschaftlicher Disziplinen entlehnt, einschließlich dem Bereich der Human-Computer Interaction, der Usability-Forschung, Marketing, der Informationstechnologíe, der Mathematik, der Linguistik und der Rechtswissenschaft. Auch kommerzielle, selbstverwaltete und staatliche Initiativen, die sich zum Ziel gesetzt haben, das Konsumentenvertrauen in eCommerce zu stärken, werden diskutiert.

Keywords: Vertrauen, Datenschutz, Security, eCommerce, Reputationssysteme, Zahlungsintermediäre, Gütezeichen, Kryptographie, digitale Signaturen, mathematische Vertrauensmodelle, Konversationsagenten, alternative Streitschlichtungsmechanismen.

1. Einleitung

Vertrauen ist ein Katalysator für zwischenmenschliche Kooperation, ermöglicht spontane soziale Interaktionen und reibungslose ökonomische Abläufe. Ein Mangel an Vertrauen wirkt wie Sand im sozialen Getriebe, weil dann Zeit und Ressourcen in Maßnahmen investiert werden müssen, die vor möglichem Schaden bewahren sollen. Das führt schließlich zu einer Verstopfung ökonomischer Prozesse. Fukuyama (1995) hat beschrieben, welche Rolle gegenseitiges Vertrauen beim Aufbau sozialer Strukturen spielt. Aber auch Misstrauen kann ein nützlicher „Geisteszustand“ sein, weil es davor bewahren kann, Schaden durch unzuverlässige Systeme oder unredliche Personen und Organisationen zu erleiden.

Konsumenten nehmen das Web als chaotische Welt wahr, die einerseits Chancen andererseits aber auch Gefahren bietet (Cheskin Research & Studio Archetype/Sapient, 1999). Zu den Faktoren, die das Konsumentenvertrauen in

---

[1]Appears in Petrovic, O. *et al.* (editors): *Trust in the Network Economy*, Evolaris Vol.2, ISBN 3-211-06853-8 Springer-Verlag, 2003.

[2] The work reported in this paper has been funded in part by the Co-operative Research Centre for Enterprise Distributed Systems Technology (DSTC) through the Australian Federal Government’s CRC Programme (Department of Industry, Science & Resources).

eCommerce beeinflussen zählen Sicherheitsrisken, Datenschutzprobleme und mangelnde Zuverlässigkeit von eCommerce-Prozessen im allgemeinen. Verschiedenen Studien und Berichte von Konsumentenorganisationen und Regierungsstellen zeigen, dass einige dieser Befürchtungen wohlbegründet sind. Im Rahmen einer Studie von „Consumers International“ (1999) führten Forscher aus elf Ländern insgesamt 151 Bestellungen auf Websites in 15 Ländern durch. Neun Prozent der Waren wurde nie ausgeliefert, in 20 Prozent der Fälle war der Rechnungsbetrag höher als erwartet und bei 21 Prozent der Bestellungen gab es Probleme mit der Rückerstattung, obwohl die fraglichen Websites mit einem Rückgaberecht geworben hatten. Die US Federal Trade Commission meldet einen rasanten Anstieg der Fälle von Online Betrug und von Konsumenten, die sich über Täuschung beklagen. Im Jahr 1997 gab es weniger als 1000 Beschwerden, im Jahr 2000 war diese Zahl auf mehr als 25.000 angestiegen (US FTC, 2001). Außerdem wurde gezeigt, dass einerseits die mediale Aufmerksamkeit in Bezug auf Sicherheitsrisken und Online Betrug die entsprechenden Ängste der Konsumenten noch verstärkt, andererseits aber die Bedenken gerade bezüglich der Sicherheit von Kreditkarteninformationen auf irrationale Weise aufgebauscht sind (Pichler, 2000).

In diesem von Risken und Unsicherheit geprägten Umfeld müssen eCommerce-Betreiber Strategien zum Aufbau von Vertrauen entwickeln sowie Systeme, die Konsumenten dabei unterstützen, das Ausmaß an Vertrauen zu bestimmen, das sie in eine spezifische eCommerce-Transaktion investieren sollen. In diesem Artikel wird eine Auswahl an Technologien und Strategien präsentiert, von denen wir meinen, dass sie ein entsprechendes Entwicklungspotenzial aufweisen.

Elemente des Web-Interface, einschließlich Gütezeichen, werden in Bezug auf ihren Effekt auf die wahrgenommene Vertrauenswürdigkeit einer Website diskutiert, Anonymisierungsverfahren, Treuhandsysteme, Versicherungsdienstleistungen und alternative Streitschlichtungsverfahren als vertrauensbildende Mechanismen zur Erhöhung des Systemvertrauens (McKnight und Chervany, 1996), die die Wahrscheinlichkeit, dass ein Konsument in eine eCommerce-Transaktion eintritt aufgrund des Vertrauens in die eCommerce-Infrastruktur - aber unabhängig vom Vertrauen in den spezifischen eCommerce-Anbieter - erhöhen. Reputationssysteme, mathematische Vertrauensmodelle und – in gewisser Weise – auch Gütezeichen sowie das „Platform for Privacy Project“ des W3C werden hinsichtlich ihres Potenzials untersucht, Konsumenten dabei zu unterstützen, informiertere Entscheidungen hinsichtlich der Vertrauenswürdigkeit ihrer eCommerce-Interaktionen zu treffen. Security-Strategien werden in Hinblick auf ihre zentrale Bedeutung für die Verbesserung der tatsächlichen Vertrauenswürdigkeit von eCommerce-Interaktionen analysiert. Besonders hervorgehoben werden aktuelle Arbeiten über Konversationsagenten als ein Forschungsgebiet, das wertvolle Beiträge zur Verbesserung künftiger eCommerce-Interfaces leisten könnte.

2. Vertrauen und eCommerce-Transaktionen

Es gibt bereits eine ganze Reihe von Modellen, die den Aufbau und die Aufrechterhaltung von Vertrauen im eCommerce-Kontext beschreiben. Die Vertrauensstudie von Cheskin Research & Studio Archetype/Sapient (1999) beschreibt Vertrauen als dynamischen Prozess, der sich als Funktion von Erfahrung vertieft oder zurückbildet. Demnach konzentrieren sich Konsumenten, sobald sie ein

gewisses Gefühl von Sicherheit erworben haben, auf fünf vertrauensbildende Signale: Marke, Navigation, Leistungserfüllung, Präsentation und Technologie. Nielsen (1999) betont, dass sich wirkliches Vertrauen aufgrund des tatsächlichen Verhaltens eines Unternehmens über die Zeit herausbildet. Vertrauen ist demnach schwierig aufzubauen und leicht zu verlieren (Nielsen u.a., 2000).

Das von Egger und de Groot erarbeitete Vertrauensmodell für eCommerce (MoTEC) (2000) kennt vier Hauptkomponenten: Faktoren, die das Vertrauen vor dem Besuch einer Website beeinflussen, wie die Reputation der Marke, frühere Offline-Erfahrungen mit dem Anbieter sowie individuelle Unterschiede hinsichtlich der allgemeinen Vertrauensdisposition; Interface-Eigenschaften wie graphisches Design und Layout, Content-Strukturierung und Usability; informationelle Inhalte, etwa Informationen, die der Anbieter über seine Produkte und Dienstleistungen zur Verfügung stellt, über Datenschutzstrategie und –praxis und schließlich das Beziehungsmanagement, das die After-Sales-Kommunikation sowie das Kundenservice umfasst.

Da Vertrauen auf Grund von Erfahrungen über die Zeit aufgebaut wird, kann der Aufbau von initialem Vertrauen für neue Anbieter im eCommerce eine große Herausforderung darstellen, vor allem für solche, die über keine etablierten offline Marken verfügen (Pichler, 2000). Ohne initiales Vertrauen können Händler keine solide Transaktionsgeschichte aufbauen – und ohne Transaktionsgeschichte ist auch der Vertrauensaufbau durch die Konsumenten erschwert. Pichler (2000) beschreibt, inwieweit sich Händler Vertrauen durch Werbung erkaufen können: Dieser Beweis für eine finanzielle Investition impliziert für den Konsumenten, dass es ein Unternehmen nicht auf eine Täuschung anlegt, um schnelle Gewinne zu erzielen. Dennoch werden die Eintrittsbarrieren gerade für kleine und mittlere Unternehmen hoch bleiben, solange keine effektiven vertrauensfördernden Mechanismen zur Erhöhung des Systemvertrauens entwickelt werden. Einige dieser neuen beziehungsweise entstehenden vertrauensfördernen Dienste werden in diesem Artikel im Überblick dagestellt.

Pichler (2000) beschreibt eCommerce-Transaktionen außerdem als Ferntransaktionen, die sehr viele Gemeinsamkeiten mit Katalog- und Telefonbestellungen aufweisen. Ferntransaktionen stellen häufig nur unzureichende Informationen über den Verkäufer und die angebotenen Waren und Dienstleistungen zur Verfügung. Er unterstreicht dabei auch die Tatsache, dass sie vom Konsumenten verlangen, das „Risiko vorgezogenen Leistungsverhaltens“ und damit eine Position der Verwundbarkeit zu akzeptieren (Pichler, 2000). Grundsätzlich hat der Konsument keine Möglichkeit, die Produkte zu sehen oder anzugreifen oder eine Dienstleistung vor der Kaufentscheidung im Detail zu evaluieren. Oft fehlen sogar Informationen über den physischen Ort, an dem der Händler zu erreichen ist, und naturgemäß auch die Körpersprache und Gestik des Kundenservicepersonals (Pichler, 2000). Die Ferntransaktionen inhärenten Defizite geben andererseits wertvolle Hinweise für die Entwicklung von Strategien zur Kommunikation von Vertrauen über Web-Interfaces sowie ganz allgemein zum Aufbau von Vertrauen in den eCommerce.

3. Kommunikation von Vertrauen über das Web-Interface

Eine Reihe von Untersuchungen hat sich mit dem Einfluss von Web-Interface-Eigenschaften auf die von den Nutzern wahrgenommene Vertrauenswürdigkeit beschäftigt. Eine von Fogg u.a. (2001a) durchgeführte quantitative Studie beschreibt, auf welche Weise 51 identifizierte Gestaltungselemente die Wahrnehmung der Nutzer in Bezug auf die Glaubwürdigkeit einer Website beeinflussen. Die Autoren schlagen vor, im Rahmen des Website-Designs die „Realkoordinaten" des Anbieters zu kommunizieren, etwa durch die genaue physische Adresse des Unternehmens und qualitativ hochwertige Bilder der Angestellten; die Website benutzerfreundlich zu gestalten; die Kompetenz des Anbieters zu belegen, zum Beispiel durch die Angabe der Qualifikationen eines Autors; den ehrlichen und unbefangenen Charakter einer Website zu kommunizieren, indem auch Links zu externen Quellen gesetzt werden; das Nutzererlebnis maßzuschneidern; amateurhafte Designfehler wie etwa typographische Fehler oder tote Links zu vermeiden; allzu kommerzielle Design-Elemente zu vermeiden, indem zwischen Werbung und tatsächlichem Content klar differenziert wird (die Resultate der Studie legen nahe, dass der letztgenannte Faktor die wahrgenommene Glaubwürdigkeit insgesamt am stärksten beeinflusst).

Eine weitere Studie von Fogg u.a. (2001b) hat herausgefunden, dass Banner-Werbung von weniger angesehenen Anbietern einen weitaus destruktiveren Effekt auf die Glaubwürdigkeit von Web-Content hat als Banner-Werbung von hochangesehenen Anbietern bzw. dass qualitativ hochwertige Fotografien der Autoren die Glaubwürdigkeit stärker erhöhen als eine Autorenzeile.

Auch die „E-Commerce User Experience" Studie der Nielsen Norman Group (Nielsen u.a. 2000) empfiehlt eine Reihe von Maßnahmen zum Aufbau von Vertrauen. Darunter: leicht auffindbare Informationen zum anbietenden Unternehmen; Preise, einschließlich Steuern und Versandkosten, bereits in einer frühen Interaktionsphase; ausgewogene Information über die Produkte; professionelles Webdesign mit verständlichen Fehlermeldungen; eindeutige und freundliche Datenschutz-, Sicherheits- und Rückgaberichtlinien; kein unverhältnismäßiges Sammeln persönlicher Informationen und klare Erklärungen darüber, wofür diese Daten benötigt werden; alternative Bestellmöglichkeiten; Möglichkeit, den Kundendienst via E-Mail oder Live Chat zu kontaktieren.

Aus der Cheskin/Sapient Studie (1999) geht hervor, dass es einer effektiven Navigation zur Kommunikation von Vertrauen in eCommerce-Websites bedarf, und dass die Qualität der Navigation von den Konsumenten als Maßstab dafür herangezogen wird, in welchem Ausmaß eine Website ihre Bedürfnisse erfüllt. Die Studie geht auch der Frage nach, inwieweit Marken oder Gütezeichen eine Rolle in Hinblick auf die wahrgenommene Vertrauenswürdigkeit spielen.

4. Datenschutz-Strategien

Verschiedene Umfragen haben gezeigt, dass der Schutz der Privatsphäre das wichtigste Anliegen der Internet-Nutzer ist (Cavoukian und Crompton, 2000). Die US Federal Trade Commission zählt zu den die Privatsphäre berührenden Beschwerden solche bezüglich unverlangt zugesendeter E-Mails, Identitätsdiebstahl, belästigende Telefonanrufe und den Verkauf von Daten an Dritte (Mithal, 2000).

Einen Versuch, diese Bedenken zu adressieren, stellt das „Platform for Privacy Preferences"-Projekt (P3P) des W3C dar (Cranor u.a., 2002). P3P ermöglicht es

Websites, ihre Datenschutzpraktiken in Form eines standardisierten, XML-basierten Formats zu kommunizieren, das von einem Webbrowser automatisch interpretiert werden kann. Ziel ist es, Widersprüche zwischen den Praktiken einer Website und den vom Nutzer gewählten Präferenzen automatisch aufzuzeigen. Obwohl es schwierig ist vorherzusagen, in welchem Ausmaß sich die P3P-Spezifikation bei eCommerce-Websites durchsetzen wird, ist es doch interessant, dass die letzte Version des Internet Explorer von Microsoft (Vs. 6.0) P3P unterstützt (Benner, 2001). P3P umfasst neun unterschiedliche Aspekte des Online Datenschutzes, von denen fünf solche Daten betreffen, die im Zuge der Nutzung einer Site mitgeloggt werden: Wer sammelt die Daten; welche Informationen werden gesammelt; zu welchem Zweck werden sie gesammelt; welche Informationen werden an andere weitergeleitet; wer erhält die Daten letztlich. Die übrigen vier Aspekte erklären die Site-internen Datenschutzstrategien: Können die Nutzer beeinflussen, für welche Zwecke ihre Daten verwendet werden; wie werden Streitigkeiten gelöst; welche Strategie verfolgt der Anbieter in Bezug auf die Speicherung der Daten; wo können detaillierte Informationen über die Datenschutzstrategie des Anbieters in einer auch für Laien verständlichen Form abgerufen werden.

P3P kann aber weder dafür garantieren, dass die Datenschutzerklärung der Website-Betreiber auch der tatsächlichen Praxis entspricht noch kann P3P Erklärungs-konformes Verhalten erzwingen. Das W3C hat aber angekündigt, dass künftige Versionen von P3P durch die Aufnahme von XML-Signaturen die Nachvollziehbarkeit von Vereinbarungen zwischen Nutzern und den Betriebern einer Website ermöglichen sollen. Künftige Versionen könnten außerdem Mechanismen integrieren, durch die Nutzer-Agenten die Bedingungen für den Transfer personenbezogener Daten verhandeln könnten. Trotz dieses Potenzials gibt es kritische Stimmen, die meinen, P3P gehe in Bezug auf Datenschutz nicht weit genug. Ziel von Datenschutz-Technologien sollte es vielmehr sein, auch anonyme Transaktionen zuzulassen (Dutton, 2000).

Zugleich entstehen private Dienstleister im Bereich des Datenschutzes, sogenannte „Anonymiser“ (The Economist, 2000). Ein Beispiel für einen Anonymisierungsdienstleister ist iPrivacy, ein Unternehmen mit Sitz in New York, das auf seiner Website erklärt, „dass nicht einmal iPrivacy die wirkliche Identität der Nutzer ihres Services kennt“. Um die Technologie zu nutzen, müssen die Nutzer zunächst eine Software von der Website eines Unternehmens, dem sie vertrauen (zum Beispiel einer Bank oder eines Kreditkartenunternehmens), herunterladen. Wenn sie dann ein Produkt online erwerben wollen, verwenden sie die Software dazu, eine einmalige fiktive Identität (Name, Adresse und E-Mail-Adresse) zu generieren. Der Nutzer hat die Wahl, die Ware selbst beim lokalen Postamt abzuholen (die Postleitzahl ist die einzige korrekte Adressinformation) oder sie sich von einem Transport- oder Postdienstleister zustellen zu lassen, dem zuvor ein dekodiertes Adresslabel geschickt wurde. In seiner ursprünglichen Version hat iPrivacy eine einmalige Kreidtkartennummer für jede Transaktion generiert. Der Kreditkartenaussteller hat daraufhin die Nummer, die er vom Händler erhalten hat, mit der echten Kreditkartennummer abgeglichen und die Zahlung autorisiert. Diese Vorgangsweise hat sich allerdings für Banken als schwer integrierbar erwiesen, daher bietet iPrivacy diese Dienstleistung mittlerweile nicht mehr an. Andere Unternehmen wie Orbiscom und Cyota bieten einmalige Kreditkartennummern weiterhin an, diese finden aber derzeit noch kaum Anwendung.

Eine weiterer Typ von Datenschutzdienstleistern oder Infomediären bildet sich in Form von Unternehmen heraus, die aggregierte Kundendaten an die Marketingabteilungen anderer Unternehmen verkaufen, die personenbezogenen Daten aber geheim halten (The Economist, 2000). Ein Beispiel für ein derartiges Unternehmen ist Lumeria, ein Unternehmen mit Sitz in Berkley, das Nutzern des Systems ihre Teilnahme vergütet. Die Nutzer laden zunächst gratis Software herunter, die ihr Profil verschlüsselt und auf den Lumeria-Servern speichert. Der Internetzugang läuft daraufhin über einen Proxy Server von Lumeria, der die Identität des Nutzers vor Online-Händlern verbirgt, gleichzeitig aber die Zusendung von Werbematerial ermöglicht, das dem Profil des Nutzers entspricht.

Um maximale Wirkung zu erzielen, müssen technologische oder selbst-regulierende Datenschutzlösungen aber in einen adäquaten rechtlichen Rahmen eingebettet sein. Gerade in der USA, dem Motor des weltweiten eCommerce, fehlt aber eine strenge und verpflichtende Datenschutzgesetzgebung (Cavoukian und Crompton, 2000). Im globalen eCommerce-Kontext wird Konsumentenschutz solange eine Herausforderung bleiben, solange es eine derartige Vielfalt nationaler Datenschutzgesetzgebungen gibt.

5. Selbstregulierung und Gütezeichen

Es gibt bereits eine Reihe von Gütezeichen, die entwickelt wurden, um über das Web-Interface Vertrauen in die Praktiken und Verfahrensweisen von eCommerce-Anbietern aufzubauen. Ein Bespiel dafür ist TRUSTe, das die Datenschutzerklärung einer Website überprüft und dieser Site gestattet, das TRUSTe-Gütesiegel zu führen, wenn die verfolgte und offengelegte Datenschutzpolitik spezifischen Standards entspricht. BBBOnline verfügt über ein ähnliches Gütezeichen und bietet außerdem einen Sicherheitsmechanismus in Form eines Streitschlichtungsprozesses an. Das CPA WebTrust-Siegel wurde von Wirtschaftsprüfern in Kanada und den USA entwickelt. Ursprünglich sollte das Gütezeichen die Datenschutz-, Sicherheits- und Geschäftspraktiken einer Site zertifizieren, einschließlich der Bestell-, Versand- und Rückgabeprozesse. Trotz der Versuche professioneller Wirtschaftsprüfer, das Gütezeichen auch in Australien einzuführen, konnte WebTrust dort keinen größeren Marktanteil erobern. Der eCommerce-Markt in Australien ist relativ klein und einige Website-Betreiber haben kritisiert, das Gütezeichen sei für ihre Bedürfnisse zu wenig flexibel. In Reaktion auf den Markt sind die meisten der großen Wirtschaftsprüfungsunternehmen dazu übergegangen, als Alternative individuelle Online-Versicherungsmodule zur Auswahl anzubieten. Die populärsten Module sind Sicherheit und Datenschutz. Ähnlich dem CPA WebTrust-Zeichen wird die Site auf Basis eines vom Anbieter vorzulegenden Online Berichts alle 90 Tage überprüft.

Aus der Cheskin/Sapient-Studie (1999) geht hervor, dass Konsumenten einer Website jedenfalls stärker vertrauen, wenn sie das dort integrierte Gütezeichen erkennen. Obwohl es sich dabei um kein Gütezeichen handelt, wurde das VeriSign-Logo von einem Drittel der Befragten dieser Studie erkannt. Von diesen erklärten mehr als die Hälfte, dass das Logo ihr Vertrauen in die Website erhöhen würde. Dieser Effekt lässt sich mit der Transferenz von Vertrauen über das vom Händler geführte Zeichen erklären. Eine spätere Studie (Cheskin, 2000) fand heraus, dass Gütezeichen in Lateinamerika und Brasilien, wo diese Gütezeichen weitgehend unbekannt sind, nur zu einer geringen Vertrauenssteigerung führten. Ähnlich wie

P3P stellen schließlich auch Gütezeichen keine Garantie dafür dar, dass die von Online-Anbietern veröffentlichten Datenschutzerklärungen auch ihrer tatsächlichen Praxis entsprechen. Die Anbieter von Gütezeichen werden selbst nicht von unabhängiger dritter Seite überwacht und vertreten daher stärker die Interessen der Branche als die der Konsumenten (Cavoukian und Crompton, 2000).

6. Sicherheitsstrategien

Die große Internet-Innovation, die über die letzten zehn Jahre zur eCommerce-Revolution geführt hat, war das Resultat einer offenen und flexiblen Netzwerkumgebung mit immer größerer Bandbreite und Funktionalität. Unglücklicherweise hat das auch eine Reihe von Sicherheitsrisiken geschaffen, die eine Gefahr für Nutzer und Online-Händler darstellen. Es ist bekannt, dass Vertrauen in digitale Transaktionen nur dann aufgebaut werden kann, wenn die Konsumenten ein Gefühl von Sicherheit haben und seitens der Betreiber beträchtliche Anstrengungen in die Entwicklung und Implementierung sicherer Services gelegt werden. Was jedoch oft übersehen wird, ist, dass es einen Trade-Off zwischen Funktionalität und Sicherheit gibt. Die eCommerce-Branche wird vor allem durch Funktionalität getrieben, Sicherheit wird folglich oft als Hindernis für eCommerce-Innovation angesehen (Fontana, 2000). Aus ökonomischer Sicht ist die derzeitige Unsicherheit kommmerzieller Systeme daher absolut rational, zugleich höchst unerwünscht aus Sicht der Nutzer (Andersen, 2001, p. 519). Um einerseits das Bedürfnis nach Vertrauensaufbau zu befriedigen, andererseits aber Innovation zu fördern, besteht die Gefahr, dass die eCommerce-Branche eher „wahrgenommene“ Sicherheit befördert statt „wirkliche“ Sicherheit zu garantieren.

Wichtige Anforderungen in Bezug auf eCommerce-Sicherheit sind das Bedürfnis, vertrauliche Informationen, die vor und nach einer eCommerce-Transaktion auf einem Computer gespeichert werden, zu schützen, die Identität des Transaktionspartners zu verifizieren, zu garantieren, dass niemand die im Zuge einer Transaktion ausgetauschten Informationen abfangen kann, und grundsätzlich die Störung der Services und Applikationen zu verhindern. Nur eine dieser Anforderungen isoliert zu befriedigen (zB Kommunikationssicherheit ohne Systemsicherheit) hat oft nur beschränkten Wert, da die gesamte Kette von Sicherheitsmaßnahmen nicht stärker sein kann als ihr schwächstes Glied. Der Sicherheitsexperte Gene Spafford hat das auf folgende Weise veranschaulicht: „Verschlüsselungstechnologien im Internet zu verwenden ist so als ob man einen gepanzerten Wagen dazu verwendete, Kreditkarteninformationen von jemandem, der in einer Kartonschachtel wohnt, zu jemandem zu bringen, der auf einer Parkbank lebt.“

Obwohl über das Internet übermittelte Daten abgefangen werden können, behaupten Forscher, dass kryptographische Kommunikationssicherheit – richtig eingesetzt – als Schutzmaßnahme für „alle Fälle mit Ausnahme der in höchstem Maße kriminell motivierten“ (Dutton, 2000) ausreicht. Wie wichtig Systemsicherheit ist, lässt sich am besten durch die Tatsache belegen, dass praktisch alle Angriffe gegen eCommerce-Server gerichtet sind. Systemsicherheit kann durch die Installation von Firewalls und Intrusion Detection Systemen, durch das Überwachen von Sicherheitsalarmmeldungen und die unmittelbare Implementierung von Sicherheitspatches erreicht werden. Das erfordert allerdings qualifizierte

Systemadministratoren, die sich laufend um die Systeme kümmern, eine sehr arbeitsintensive Tätigkeit.

Die Probleme der Authentifizierung eines Online Transaktionspartners und der Nachweisbarkeit von Transaktionen können theoretisch durch Public-Key-Verschlüsselung gelöst werden. Es wird prognostiziert, dass bald jede Organsiation und jede Person im Internet ihr eigenes Paar aus öffentlichem und privatem Schlüssel als Basis ihrer digitalen Identität besitzen wird. Das setzt die sichere Erzeugung und Verteilung von möglicherweise mehreren Hundert Millionen Schlüsselpaaren voraus, was erhebliche Schlüssel- und Vertrauensmanagementprobleme mit sich bringt. Private Schlüssel müssen von ihren Inhabern sicher verwahrt werden. Öffentliche Schlüssel werden in öffentlichen Hinterlegungsstellen gespeichert und als Public-Key-Zertifikate verteilt, die von einer Zertifizierungsstelle signiert sind. Zertfizierungsstellen muss man vertrauen können, dass sie die Identifizierung der Schlüsselinhaber gründlich durchführen und Schlüsselbesitzern muss man das Vertrauen entgegenbringen, dass sie ihre privaten Schlüssel sicher verwahren. Was aber, wenn eine Zertifizierungsstelle ein Zertifikat ausstellt, ohne die Identität des Inhabers ordnungsgemäß überprüft zu haben? Das war der Fall, als die weltweit größte Zertifizierungsstelle VeriSign falsche Zertifikate auf Microsoft ausgestellt hat, weil sie bei der korrekten Identifizierung der Inhaber der Zertifikate einen Fehler gemacht hat (Microsoft, 2001). Was, wenn ein privater Schlüssel gestohlen oder durch Zufall oder böse Absicht veröffentlicht wird? Da private Schlüssel oft auf Webservern aufbewahrt und diese oft und erfolgreich angegriffen werden, sind diese Schlüssel von Diebstahl und Missbrauch bedroht. Derartige Ereignisse können dazu führen, dass Systeme oder Nutzer falsche Annahmen über Identitäten treffen, vor allem weil die derzeit gängigen Webbrowser keinen Zugriff auf Zertifikatannullierungslisten haben.

Sowohl menschliche Faktoren als auch User Interfaces stellen heute für die Informationssicherheit besonders große Herausforderungen dar. Die Effektivität an sich sicherer Systeme wird regelmäßig durch einfache Sozialtechniken vereitelt (Andersen, 2001 p. 37 und Lemos, 2000). Um solchen Angriffen standzuhalten, muss daher das Design von eCommerce-Systemen so robust wie möglich sein. Eine der wenigen Publikationen, die sich empirisch mit User-Interface-Problemen im Bereich technischer Sicherheit befassen, ist „Why Johnny can´t Encrypt: A Usability Evaluation of PGP 5.0“ (Whitten und Tygar, 1999). Dabei wird das User Interface von PGP (Zimmermann, 1995) nach allgemeinen Richtlinien als gut bewertet. Dennoch kommen die Autoren zum Schluss, dass PGP 5.0 in Bezug auf die Usability nicht geeignet ist, dem durchschnittlichen Computernutzer effektive Sicherheit zu bieten. Sie argumentieren, dass es eines speziellen Usabilitystandards für technische Sicherheit bedarf und dass gängige Software-Interfacedesign-Techniken für Belange technischer Sicherheit nicht brauchbar sind (Whitten und Tygar, 1999). Da die meisten Sicherheitslücken auf menschliches Versagen zurückzuführen sind, müssen die humanzentrierten Faktoren im Zusammenhang mit Fragen der technischen Sicherheit künftig stärker zu beachten.

7. Mathematische Vertrauensmodelle

Formale Vertrauensmodelle sind vor allem in der Information Security Community Gegenstand der Forschung. Vertrauensmodelle wie beispielsweise das von PGP

(Zimmermann, 1995), Maurer (1996), Abdul-Rahman und Hailes (1997) und Jøsang (1999) beschäftigen sich hauptsächlich mit der Frage des Vertrauens in die Identität von Instanzen unter Verwendung kryptographischer Mechanismen, um Maßzahlen für Vertrauen zu propagieren. Diese Modelle können außerdem dazu verwendet werden, Vertrauen in Instanzen selbst abzuleiten und bieten dadurch eine ähnliche Art von Evidenz wie Reputationssysteme.

Menschen fällt es in der Regel schwer, numerische Vertrauensmaße zu bestimmen, die als Input benötigt werden. Eine Annäherung an dieses Problem ist die Verwendung einer Reihe verbaler Kennzeichnungen - zum Beispiel *starkes Vertrauen, schwaches Vertrauen, ungewisses Vertrauen, schwaches Misstrauen und starkes Misstrauen* -, mit denen das System dann entweder direkt arbeitet (wie bei PGP) oder das es zuvor in numerische Werte übersetzt. Derartige Vertrauensmodelle zielen darauf ab, die Ableitung von Vertrauensmaßgrößen sowohl intuitiv verständlich als auch mathematisch korrekt zu gestalten. Ziel ist es, Systeme zu entwickeln, die fähig sind, automatisch und auf menschenähnliche Weise über Vertrauen zu urteilen, zugleich aber nicht anfällig sind für Manipulationen und die für Menschen typischen Urteilsfehler. Es bedarf noch praktischer Umsetzungen sowie empirischer Tests, um die Adäquatheit dieses Ansatzes zu bestimmen.

8. Zahlungsintermediäre und Versicherungsdienstleister

Zahlungsintermediäre sind in eCommerce-Transaktionen oft die einzigen Parteien, die Identität und Standort des Händlers verifizieren können (Pichler, 2000). Pichler behauptet, dass Kreditkartenunternehmen auf Grund dieser Tatsache eine einflussreiche Position erlangt haben. So können sie etwa betrügerische Händler, die in Bezug auf Auszahlungen auf sie angewiesen sind, von ihren Dienstleistungen abschneiden. Pichler tritt dafür ein, die Rolle von Kreditkartenunternehmen auszuweiten und sieht Möglichkeiten, neue Formen von Zahlungsintermediären zu entwickeln, um das Vertrauen in digitale Transaktionen zu erhöhen. Zahlungsintermediäre können Konsumenten dadurch unterstützen, dass sie deren „Risiko vorgezogenen Leistungsverhaltens“ mildern, das den Konsumenten in der Regel in eine Position der Verwundbarkeit bei digitalen Transaktionen versetzt (Pichler, 2000). Zahlungsintermediäre können neue Händlern außerdem beim Aufbau initialen Vertrauens helfen.

Treuhand-Dienstleister stellen eine spezifische Form von Zahlungsintermediären im B2C, C2C und B2B-eCommerce dar. Sie halten die Zahlung des Käufers solange zurück, bis dieser die Waren erhalten und akzeptiert hat. Erst dann wird die Zahlung an den Verkäufer freigegeben. Außerdem entstehen neue Arten von Kreditkarten, die den Konsumenten Online-Shopping-Garantien bieten. „Amex Blue“ zum Beispiel bietet an, den Kaufpreis zu erstatten, wenn der Konsument mit den Waren unzufrieden ist, unabhängig davon, ob der Internet-Anbieter eine derartige Rückerstattung anbietet. Es gibt allerdings eine Erstattungsgrenze von 300 $ pro Kauf bzw. von 1000 $ pro Jahr. Weiters entwickeln sich Versicherungsunternehmen, die eCommerce-Transaktionen versichern. Das deutsche Versicherungsunternehmen Gerling zum Beispiel bietet teilnehmenden eCommerce-Sites eine derartige Versicherung sowie das „Trusted Shop“-Gütesiegel (Pichler, 2000).

9. Reputationssysteme

Reputationssysteme haben sich als weitere Methode herausgebildet, im eCommerce-Kontext Vertrauen unter Unbekannten aufzubauen. Ein Reputationssystem sammelt, verteilt und aggregiert Feedback über das Verhalten der Teilnehmer. Resnick u.a. (2000) meinen, dass diese Mechanismen Nutzer bei der Entscheidung, wem sie vertrauen sollen, unterstützen können und Anreize für ehrliches Verhalten bieten. Außerdem können sie dazu beitragen, unehrliche Parteien von der Teilnahme abzuhalten.

Frühere Erfahrungen mit einem Online-Transaktionspartner werden dabei in die Zukunft projiziert; daraus ergibt sich eine Maßgröße für deren Vertrauenswürdigkeit. Der Politikwissenschafter Robert Axelrod (1984) hat diesen Effekt den „Schatten der Zukunft“ genannt. Wenn Fremde in eCommerce-Settings ohne derartige Systeme miteinander in Interaktion treten, könnte die Versuchung, für kurzfristige Gewinne betrügerisch zu handeln, attraktiver sein als Kooperation. Die ersten Websites, die Reputationssysteme eingeführt haben, waren Online Auktionssites wie eBay. Heute werden sie auch von Ratingsites für die Reputation von Unternehmen wie BizRate eingesetzt, die Web-Händler auf Basis von Kundenratings reihen. Die eRatings von Consumer Reports Online reihen Händler auf Grund von Testkäufen, die Mitarbeiter von Consumer Reports durchführen. Außerdem sind Websites für Produkt-Reviews, wie Epinions.com, entstanden, wo die Produkttests selbst von anderen Reviewern bewertet werden. Mit der Ausnahme von eRatings treffen die meisten Systeme kaum Vorkehrungen für das Problem des Aufbaus von initialem Vertrauen in neue eCommerce-Anbieter, da starke Reputationssysteme sich normalerweise erst über die Zeit entwickeln (Pichler, 2000).

In der physischen Welt kann das Sammeln und Verteilen von Feedback zu einer kostspieligen Angelegenheit werden. Das Internet ist im Vergleich dazu extrem effizient. Dennoch stehen Reputationssysteme vor einer Reihe signifikanter Herausforderungen. Wenn eine Instanz ihren Namen ändert, kann Feedback auch gelöscht werden, und ein unehrlicher Teilnehmer kann auf diese Weise immer dann von Neuem beginnen, wenn er eine schlechte Reputation aufgebaut hat. Darüber hinaus kann es schwierig sein, Nutzer überhaupt zur Abgabe von Feedback zu motivieren - besonders zu negativem Feedback -, und sicherzustellen, dass das Feedback aufrichtig war (Resnick u.a., 2000). Ein Beispiel für einen unredlichen Missbrauch eines Reputationssystems war der Versuch von drei Männern, auf eBay ein gefälschtes Gemälde um 135,805 $ zu verkaufen (Young, 2001). Der Verkauf wurde erst unmittelbar vor Abschluss abgebrochen, da der Käufer Verdacht schöpfte. Es stellte sich heraus, dass zwei der Betrüger gute Ratings im Feedback Forum hatten, die daraus entstanden waren, dass die beiden sich gegenseitig positiv bewertet und vor dem Betrugsversuch ehrliche Verkäufe durchgeführt hatten. Reputationssysteme weisen somit ein Vielzahl komplexer Facetten auf und entwickeln sich zu einem fruchtbaren Forschungsgebiet[3].

10. Humanoide

[3] Das Reputation System Network ist ein Forschungsforum für Wissenschafter, die sich damit beschäftigen, wie Reputationssysteme theoretisch und praktisch funktioneren sollten und wie man sie verbessern könnte (http://databases.si.umich.edu/reputations).

Sprachwissenschafter, die ein Verständnis davon haben, wie Vertrauen über Konversationsrituale aufgebaut wird, arbeiten zusammen Informatikern an der Entwicklung Computer-generierter Agenten in Menschen-ähnlicher Form mit der Fähigkeit, in einen sozialen Dialog zu treten. Sie verwenden Gestik, Blicke, Körperhaltung, Intonation und andere Elemente, um die Erfahrung persönlicher Kommunikation nachzuempfinden. Am MIT Media Lab (Bickmore und Cassell, 2001) wurden bereits Prototypen sogenannter „Embodied Conversational Agents“ entwickelt. Einer dieser Prototypen wurde eigens für online-Immobilien-Transaktionen designt. Auch Beskow und McGlashan (1997) und Van Mulken u.a. (1999) haben Studien zu Konversationsagenten verfasst.

REA - der „Real Estate Agent“ (2001) – also der Prototyp von Bickmore und Cassell, kann Small Talk führen und das Feedback seines Konversationspartners überwachen. Er kann Konversationsthemen verfolgen und Konversationsmanöver durchführen, etwa die Konversation von einem allgemeinen Gespräch über das Wetter zu einem Gespräch über das Wetter in Boston zu einer Konversation über Immobilienpreise in Boston entwickeln. Konversationen dürfen nur dann in Richtung sensiblerer Task-spezifischer Gespräche entwickelt werden, wie zum Beispiel zum Thema Wohnfläche oder gewünschter Preislage, wenn zuvor ein vordefiniertes Solidaritätsrating für dieses Thema erreicht wurde. Ein Experiment hat die Teilnehmer im Zuge der Darstellung von zwei virtuellen Apartments abwechselnd in Small Talk, der daraufhin in ein Task-spezifisches Gespräch übergeleitet wurde, oder direkt in ein Task-spezifisches Gespräch verwickelt. Die Teilnehmer haben dabei einen Fragebogen ausgefüllt, der die wahrgenommene Kompetenz gemessen hat, das persönliche Gefallen, die Intelligenz sowie ein Normalmaß an Vertrauenswürdigkeit. Die bisherigen Resultate legen nahe, dass viele Nutzer den Agenten als kompetenter, zuverlässiger und sachkundiger empfinden, wenn er zunächst Small Talk einsetzt als wenn er ausschließlich Task-spezifisch kommuniziert (Bickmore und Cassell, 2001).

11. Alternative Streitschlichtung

Auch alternative Streitschlichtungsmechanismen werden in Hinblick auf weitere Möglichkeiten zum Aufbau von Vertrauen erforscht. Die Hypothese ist, dass die Akzeptanz von eCommerce auf Konsumentenseite dann zunehmen wird, wenn die Nutzer zuversichtlich sind, dass sie Rückgriff auf einen fairen, zuverlässigen und effektiven Prozess haben, sobald ein Konflikt auftritt, der sich nicht über die normalen Kundendienstprozesse des anbietenden Unternehmens lösen lässt.

Während Befürworter alternativer Streitschlichtungsmechanismen darin übereinstimmen, dass sowohl Händlern als auch Konsumenten zu jedem Zeitpunkt der Weg zum Gericht offenstehen sollte, wird das Rechtssystem für eCommerce-Konflikte zugleich für ungeeignet erachtet (Carblanc, 2000). Probleme schließen substanzielle Prozesskosten mit ein, die oft höher als der Streitwert sind, sowie die Tatsache, dass sich Gerichtsprozesse in die Länge ziehen können. Außerdem kann es schwierig sein festzustellen, welches Recht in eCommerce-Streitigkeiten zur Anwendung kommt, welche Institution für den Fall zuständig ist und ob das Urteil in grenzüberschreitenden Fällen durchsetzbar ist. Alternative Streitschlichtung löst viele dieser Probleme. Im allgemeinen beginnt ein Streitschlichtungsverfahren, wenn eine

Partei eine Beschwerde bei einem Anbieter alternativer Streitschlichtungsverfahren einreicht, der dann seinerseits die andere Partei bzw. die anderen Parteien von der Beschwerde benachrichtigt. Darauf folgt eine Reihe von Interaktionen der Streitparteien untereinander - vermittelt von der neutralen Drittpartei -, mit dem Ziel, den Konflikt zu lösen. Alternative Streitschlichtung kann sowohl Menschen-assistiert als auch voll automatisiert ablaufen. Die Bandbreite der möglichen Verfahren reicht von unterstützten Verhandlungen, im Zuge derer eine Drittpartei die Streitparteien zu einer gemeinsamen Lösung zu führen versucht, bis hin zur Schiedsgerichtsbarkeit, wo der Sachverhalt einer Drittpartei überantwortet wird, die die endgültige Entscheidung trifft.

Mehr als 39 Online-Streitschlichtungssysteme lassen sich derzeit ausmachen (Carblanc, 2000). Allgemein anerkannte Prinzipien alternativer Streitschlichtung sind, dass sie zugänglich, zeitgerecht, neutral, freiwillig, für Konsumenten gratis oder kostengünstig sind sowie transparent in Bezug auf ihre Verfahren, Kosten und die Art der angebotenen Schlichtungsdienste. Der „Trans-Atlantic Consumer Dialogue“, ein Forum für Konsumentenorganisationen aus den USA und der EU, schlägt die Errichtung einer internationalen Clearingstelle für die Publikation von Details zu allen Streitschlichtungsfällen vor, die sowohl für Exekutivorgane als auch für die Öffentlichkeit zugänglich sein sollte (Carblanc, 2000). Der „Global Business Dialogue on Electronic Commerce“, eine internationale Gruppe von Unternehmensvorständen, hat betont, dass die Regierungen die Einrichtung alternativer Streitschlichtungsprogramm in der Wirtschaft fördern, zugleich aber davon absehen sollten, zwingende Zulassungsverfahren für die Anbieter solcher Programme einzuführen (Carblanc, 2000). Einige Länder wie etwa Großbritannien haben zwar kein obligatorisches System eingeführt, sehr wohl aber ein Rahmenprogramm (zB TrustUK), das Gütesiegelanbieter nur unter der Voraussetzung unterstützt, dass sie auch einen geeigneten Streitschlichtungsmechanismus vorsehen und spezielle Standards erfüllen (Bond, 2000).

Empfohlen wird auch, dass Unternehmen, die an einem Streitschlichtungsprogramm beteiligt sind, von ihrer Website zu einem oder mehreren Anbietern derartiger Verfahren verlinken mit dem deutlichen Hinweis, dass sich Kunden, die mit der Leistung nicht vollständig zufrieden sind, an dieses Streitschlichtungssystem wenden können. Auch Regierungen, Konsumentenorganisationen und Wirtschaftsverbände sollten von ihren Websites Links zu Streitschlichtungsverfahren anbieten, um Konsumenten auf der Suche nach Rechtshilfe möglichst zu unterstützen (Carblanc, 2000).

Eine der größten Herausforderungen für Systeme alternativer Streitschlichtung betrifft die Duchsetzbarkeit der Entscheidungen. Ein – auch unter Befürwortern - besonders kontroversielles Thema ist dabei, ob und unter welchen Bedingungen eine derartige Entscheidung für eine oder mehrere Parteien verbindlich sein sollte (Dorskind, 2000). In diesem Zusammenhang wurde vorgeschlagen, dass dort, wo alternative Streitschichtungssysteme von Wirtschaftsverbänden oder anderen Gruppen aus der Wirtschaft betrieben werden, die Unterwerfung unter diese Entscheidungen eine verpflichtende Bedingung für die Mitgliedschaft ist. Drittparteien, die die Abwicklung von Transaktionen unterstützen wie zum Beispiel Auktionsbetreiber oder Zahlungsintermediäre, würden dann aufgefordert, den Händlern, die sich nicht unterwerfen, ihre Dienstleistungen zu verweigern (Carblanc, 2000).

12. Künftige Forschungsarbeiten

Vertrauen und die Auswirkungen von Vertrauen auf die Akzeptanz von eCommerce stellen eine reiches Betätigungsfeld für weitere Forschung dar. Da Vertrauen ein wichtiges Thema im Zusammenhang mit Online Konsumentenverhalten ist, ist die Frage, in welchem Zusammenhang Vertrauen mit anderen Faktoren steht, wie zum Beispiel der Kaufmotivation, von großer Bedeutung. Es wäre wichtig zu analysieren, welche Strategien man zur Kommunikation von Vertrauen und Glaubwürdigkeit über ein Webinterface für verschiedene Branchen, Berufsgruppen und Unternehmen verfolgen kann und die tatsächlichen Auswirkungen dieser unterschiedlichen Strategien auf das Kaufverhalten und den Umsatz zu beschreiben und zu messen.

In vielen Ländern ist es weiters nötig, die Datenschutzgesetzgebung für den Online Kontext zu adaptieren und zu stärken, um zu gewährleisten, dass technologische oder selbst-regulierende Datenschutzlösungen größtmögliche Wirkung und Durchsetzbarkeit entfalten können. Auch künftige Versionen von PGP könnten zu einer stärkeren Durchsetzbarkeit im Bereich des Datenschutzes beitragen, und zwar wenn digitale Signaturen in die entsprechende Spezifikation aufgenommen würden, um Beweisbarkeit sicher zu stellen. Zusätzliche Forschungsarbeiten im Bereich praktischer Anwendungsmöglichkeiten für mathematische Vertrauensmodelle könnten als Grundlage für Werkezeuge dienen, die es Konsumenten ermöglichen, eCommerce-Entscheidungen auf Vertrauensbasis zu treffen.

Bessere Webinterfaces mit einer menschlichen Note und optimierter Usability könnten aus weiterführenden Forschungen im Bereich vertrauensbildender Konversationsrituale und aus der Verfeinerung der Konversationsfähigkeiten von „Embodied Conversational Agents“ hervorgehen. Während Kommunikationssicherheit relativ einfach zu erzielen ist, bedarf es noch einiger Arbeit, um auch starke Systemsicherheit für eCommerce-Nutzer leicht erzielbar zu machen. Da die meisten Sicherheitslücken durch menschliche Fehler zustande kommen, könnten sich weitere Arbeiten in den Bereichen Security Management Praktiken, Usability und Security sowie zur Verbesserung der User-Interfaces von Sicherheitstechnologien als wertvoll erweisen. Bereits erwähnt wurden laufende Arbeiten zur Verbesserung der in Reputationssystemen verwendeten Metriken. Künftig wird es darum gehen, diese Systeme gegen Manipulationen durch unehrliche Teilnehmer abzusichern.

Wenn alternative Streitschlichtungsmechanismen die in sie gesetzten Erwartungen in Bezug auf die Erhöhung von Vertrauen in den weltweiten eCommerce erfüllen sollen, wird es notwendig sein herauszufinden, wie effektiv diese Mechanismen in unterschiedlichen Kulturen wirklich sind, und neue Technologien wie Stimmerkennung und Übersetzungstechnologien in mehrsprachigen Streitfällen einzusetzen. Genauso wichtig ist auch die Beschäftigung mit neuen, in der Privatwirtschaft entwickelten Lösungen zum Vertrauensaufbau. Lösungen zum Schutz der Privatsphäre werden bereits entwickelt, und es wird interessant sein zu beobachten, in welchem Umfang sich neue, auf den eCommerce-Bereich zugeschnittene Zahlungs- und Versicherungslösungen auf dem Markt durchsetzen werden.

13. Schlussfolgerung

Wer nicht vertrauen kann, der zögert. Die mangelnde Akzeptanz von eCommerce durch die Konsumenten ist zum Teil auf einen Mangel an Vertrauen in eCommerce-Anbieter, in die entsprechende Technologie sowie in die Geschäftsprozesse zurückzuführen, sowie den Mangel an zuverlässigen, durchsetzbaren Systemen, die zum Einsatz kommen, wenn etwas schiefgeht. Dieser Artikel hat eine große Bandbreite von Technologien und Strategien analysiert, die versuchen, eine Lösung für diese Probleme zu finden, und einige Vorschläge für künftige Forschungsfelder vorgestellt, die hoffentlich zur Entwicklung verbesserter Werkzeuge für Konsumenten zur Einschätzung von Vertrauen und zur Steigerung des Konsumentenvertrauens in den eCommerce insgesamt führen werden.

Danksagung

Die diesem Artikel zugrundeliegenden Arbeiten wurden teilweise vom „Cooperative Research Center for Enterprise Distributed Systems Technology“ (DSTC) durch das CRC-Programm der australischen Bundesregierung (Department of Industry, Science & Resources) gefördert.

Quellenangaben

Abdula-Rahman, A. und S. Hailes: 1997, „A Distributed Trust Model“. In: *Proceedings of the 1997 New Security Paradigms Workshop*. S. 48-60, ACM.

Andersen, R.: 2001, *Security Engineering*. Wiley.

Axelrodt, R.: 1984, *The Evolution of Cooperation*. New York: Basic Books.

Benner, J.: 2001, „MS Gets Privacy-Happy With New IE”. *Wired News*. http://www.wired.com/news/privacy/0,1848,43686,00.html

Beskow, J. und S. McGlashan: 1997, „Olga: A Conversational Agent with Gestures“. In: *Proceedings of the IJCAI´97 workshop on Animated Interface Agents: Making them Intelligent*. Nagoya, Japan.

Bickmore, T. und J. Cassell: 2001, “Relational Agents: A Model and Implementation of Building User Trust”. In: *CHI 2001 Conference Proceedings*. ACM Press.

Bond, M.: 2000, „Role of stakeholders in identifying essential elements of trustmark programs, codes of conduct and dispute resolution schemes”. In: *Proceedings of the Joint Conference of the OECD, HCOPIL, ICC: Building Trust in the Online Environment: Business to Consumer Dispute Resolution* (The Hague). http://www.oecd.org/pdf/M00001000/M00001632.pdf

Carblanc, A.: 2000, „Privacy Protectionand Redress in the Online Environment: Fostering Effective Alternative Dispute Resolutions”. In: *Proceedings of the 22nd International Conference on Privacy and Personal Data Protection*.

Cavoukian, A. und M. Crompton: 2000, „Web Seals: A Review of Online Privacy Programs“. A Joint Project of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, http://www.ipc.on.ca/english/pubpres/papers/seals.pdf.

Cheskin Research: 2000, *Trust in the Wired Americas*. Cheskin Research, http://www.cheskin.com/docs/sites/1/report-CheskinTrustIIrpt2000.pdf.

Cheskin Research & Studio Archetype/Sapient: 1999, *eCommerce Trust Study*. Sapient, http://www.cheskin.com/docs/sites/1/report-eComm%20Trust1999.pdf

Consumers International: 1999, *Consumers@shopping: An international comparative study of electronic commerce*. Consumers International`s Programme for Developed Economies and Economies in Transition, http://www.consumersinternational.org/document_store/Doc504.pdf.

Cranor, L. u.a.: 2002, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. W3C Recommendation 16 April 2002, http://www.w3.org/TR/P3P.

Dorskind, J.: 2000, „Remarks to ADR by the US Department of Commerce”. In: *Proceedings of the Joint Conference of the OECD, HCOPIL, ICC: Building Trust in the Online Environment: Business to Consumer Dispute Resolution* (The Hague). http://www.oecd.org/pdf/M00001000/M00001606.pdf

Dutton, P.: 2000, „Trust Issues in eCommerce”. In: *Proceedings of the 6th Australasian Women in Computing Workshop*. S. 15-26, Griffith University.

Egger, F. und B. de Groot: 2000, „Developing a Model of Trust for Electronic Commerce: An Application to a Permissive Marketing Web Site“. In: *Proceedings of the 9th International World-Wide Web Conference*. Foretec Seminars.

Fogg, B. u.a.: 2001a, „What makes Web sites credible? A report on a large quantitative study”. In: *Proceedings of CHI 2001*. S. 61-68, ACM Press.

Fogg, B. u.a.: 2001b, „Web Credibility Research: A Method for Online Experiments and Early Study Results”. In: Proceedings of CHI 2001. S. 295-296, ACM Press.

Fontana, J.: 2000, „Outlook patch called overkill”. *Cnn.com NewsNet*. http://www.cnn.com/2000/TECH/computing/05/23/outlook.overkill.idg.

Fukuyama, F.: 1995, *Trust: The Social Virtues and the Creation of Prosperty*. The Free Press, New York.

Jøsang, A.: 1999, „An Algebra for Assessing Trust in Certification Chains”. In: J. Kochmar /ed.): *Proceedings of the Network and Distributed Systems Security Symposium (NDSS´99)*. The Internet Society.

Lemos, R.: 2000, „Mitnick teaches `social engineering´”. ZD Net News. http://zdnet.com.com/2100-11-522261.html?legacy=zdnn.

Maurer, U.: 1996, „Modelling a Public-Key Infrastructure". In: E. Bertino u.a. (eds.): *Proceedings of the Fourth European Symposium on Research in Computer Security (ESORICS´96)*. Springer.

McKnight, D. und N. Chervany: 1996, „The Meanings of Trust". Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Informations Systems Research Center, URL: http://www.misrc.umn.edu/wpaper.

Microsoft: 2001, „Microsoft Security Bulletin MS01-017 (March 22, 2001): Erroneus VeriSign-Issued Digital Certificates Pose Spoofing Hazard". http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-017.asp.

Mithal, M.: 2000, „Illustrating B2C Complaints in the Online Environment". Presentation by the US Federal Trade Commission and Industry Canada, at the Joint Conference of the OECD, HCOPIL, ICC: Building Trust in the Online Environment: Business to Consumer Dispute Resolution (The Hague). http://www.oecd.org/ppt/M00001000/M00001614.ppt.

Nielsen, J.: 1999, „Trust or Bust: Communicating Trustworthiness in Web Design". Jakob Nielsen´s Alertbox, http://www.useit.com/alertbox/990307.html.

Nielsen, J., R. Molich, C. Snyder und S. Farrell: 2000, „ECommerce User Experience". Technical Report, Nielsen Norman Group.

Pichler, R.: 2000, *Trust and Reliance – Enforcement and Compliance: Enhancing Consumer Confidence in the Electronic Marketplace*. Standford Law School, http://www.oecd.org/pdf/M00001000/M00001602.pdf.

Resnick, P. u.a.: 2000, „Reputation Systems". *Communications of the ACM* **43**(12), 45-48.

The Economist: 2000, „The Coming Backlash in Privacy". *The Economist Technology Quarterly*. December 9.

US FTC: 2001, „Boom in ECommerce has created Fertile Ground for Fraud". US Federal Trade Commission, http://www.ftc.gov/opa/2001/05/iftestimony.htm.

Van Mulken, S. und E. André und J. Müller: 1999, „The Trustworthiness of Lifelike Interface Characters". In: *Proceedings of the 8th International Conference on Human-Computer Interaction (HCI International´99)*. Munich, Germany.

Whitten, A. und J. Tygar: 1999, „Why Johnny Can´t Encrypt: A Usability Evaluation of PGP 5.0". In: *Proceedings of the 8th USENIX Security Symposium*.

Young, E.: 2001, „Not a pretty picture". *The Industry Standard* (online newsletter). http://www.thestandard.com/article/0,1902,22875,00.html.

Zimmermann, P.: 1995, *The Official PGP User´s Guide*. MIT Press.