TECHNISCHE UNIVERSITÄT ILMENAU

Vertrauen im Internet

Wie sicher soll E-Commerce sein?

Rüdiger Grimm

Nr. 01 **April 2001**

Diskussionsbeiträge

INSTITUT FÜR MEDIEN- UND KOMMUNIKATIONSWISSENSCHAFT

Vertrauen im Internet

Wie sicher soll E-Commerce sein?

Rüdiger Grimm

Nr. 01 April 2001

TU Ilmenau - Institut für Medien- und
Kommunikationswissenschaft

Vertrauen im Internet - Wie sicher soll E-Commerce sein?

Rüdiger Grimm

Technische Universität Ilmenau, Am Eichicht 1, 98684 Ilmenau
Tel 03677 69 4735, Fax 03677 69 4724, ruediger.grimm@tu-ilmenau.de

Ausgearbeitete und erweiterte Version der Antrittsvorlesung am 11.12.2000

Wird veröffentlicht zum Berliner Kolloquium, 9.5.2001, Springer 2001

Zusammenfassung

Im ersten Teil werden Sicherheitsprobleme von E-Commerce analysiert. Dabei werden besonders technische Sicherheitsprobleme des Internet behandelt. Als Folgerung daraus wird eine Liste von sieben Forschungs- und Entwicklungsaufgaben zusammengestellt. Im zweiten Teil wird eine der Forschungsaufgaben beleuchtet, nämlich die Entwicklung der Mensch-Maschine-Schnittstelle in Bezug auf die Frage, wieviel Automatisierung menschliche Kommunikation verträgt. Das erhellt das Sicherheits- und Vertrauensproblem für E-Commerce.

Teil 1: Vertrauen im Internet

Im ersten Teil werden Sicherheitsprobleme von E-Commerce analysiert und es wird der Vertrauensbegriff entwickelt.

1. E-Commerce

Zu den modernen Schlagworten, die sowohl Hoffnung auf eine bessere Zukunft als auch Angst vor einer Zerstörung gewohnter Werte wecken, gehören „Informationsgesellschaft“, „Globalisierung“ und „E-Commerce“. Man fühlt sich gedrängt: wer heute noch nicht im Internet sei, gehöre bereits zum alten Eisen und sei morgen geschäftlich tot. Gigantische Wachstumsraten an neuen Aufgabenstellungen und Arbeitsplätzen im Bereich der Informatik locken Heerscharen von Studenten in die Informatik- und Medienstudiengänge. Wirtschaft und Wissenschaft schreiben mehr Projekte aus, als von den bestehenden Experten bewältigt werden können.

Im *Privatkundengeschäft* (Business-to-Consumer, B2C) werden virtuelle Web-Portale Zweigstellen und Einzelgeschäfte überflüssig machen. Homebanking und elektronische Bücherbestellungen gehören längst zum Anwendungsalltag des Internet. Entsprechend reagieren Banken und Buchhandel bereits heute mit einer verstärkten Internet-Präsenz. Im *Firmenkundengeschäft* (Business-to-Business, B2B) werden Vertrieb und Einkauf revolutioniert, indem Geschäftsprozesse in großem Stil firmen- und länderübergreifend zusammengeschaltet werden. Zum Beispiel können sinkende Lagerbestände automatisch Bestellungen beim Zulieferer auslösen. Die Auswirkung ist offen: werden langfristig verabredete Arbeitsteilungen, so wie man es heute noch gewohnt ist, von ewigen Auktionen abgelöst, in denen der jeweils billigste Anbieter weltweit bei jedem externen Geschäftsvorgang spontan den Zuschlag bekommt? Wird die Arbeitsteilung beschleunigt oder kommt es gar zu alten Machthierarchien zurück, in welchen die stärksten Partner allen von ihnen abhängigen Kunden und Zulieferern ihre Geschäftsprozesse aufzwingen?

Welche Technik ist es, die die Fantasie eines voll-elektronischen Geschäftslebens beflügelt? Was eigentlich versteht man unter „Electronic Commerce“?

Mit *Electronic Commerce* bezeichnet man das Betreiben von Geschäften mit Hilfe neuer elektronischer Medien. Die treibenden technischen Entwicklungen der letzten Jahre sind

- das offene und globale Internet,
- die mobile Telefonie,
- die Miniaturisierung der Computer hin zu Smartcards und „Personal Digital Assistants“,
- die mathematische und technische Entwicklung der elektronischen Signatur,
- sowie die Möglichkeit zur elektronischen Zahlungsabwicklung.

Man meint mit den neuen elektronischen Medien in erster Linie das weltweite offene Internet. Kartenbasierte Bezahlvorgänge am Geldautomat, bzw. in Geschäftsräumen („Point-of-Sale“) sowie Online-Bestellungen und Home-Banking in geschlossenen Online-Diensten (T-Online, Compuserve, AOL) zählen ebenfalls zu Geschäften des Electronic Commerce. Die mobile Telefonie ist der jüngste Mitspieler in der neuen Medienwelt, der insbesondere deswegen für Zuwachs im elektronischen Privatkundengeschäft sorgen könnte, weil „Handies“ von allen Bevölkerungsschichten angenommen werden, auch von solchen, die mit dem Internet nichts anfangen wollen. All diese technisch zunächst verschiedenen Medien - das Internet mit seiner Dienstleistungsinfrastruktur, die mobilen Telefonnetze, Smartcard-Anwendungen und Online-Dienste - wachsen technisch und organisatorisch zusammen und bilden eine globale Welt des Electronic Commerce, in denen vertragsbasierte geldwerte Tauschaktionen durchgeführt werden können.

Das *Internet* und seine Sicherheitsprobleme werde ich unten genauer besprechen. Seine Standardanwendungen E-Mail und World Wide Web erlauben es, *digitale Waren* (Texte, Bilder, Software usw.) direkt und weltweit über das Internet zu verteilen.

In jüngerer Zeit beschleunigt vor allem die Akzeptanz von *Mobiltelefonie* in Europa die Hoffnung elektronischer Geschäftsanbieter, Privatkunden über Mobiltelefone an ihre Angebote im WWW anzuschließen. Die Milliardenerlöse bei der Versteigerung der UMTS-Lizenzen in ganz Europa im Jahre 2000 sind ein Indiz für die Zukunftserwartung in mobilen E-Commerce. Die (mindestens zeitweilige) Popularität der einfachen WAP-Technik ist ein anderes Indiz für die Hoffnung, schon kurzfristig Kunden mit ihren heutigen GSM-Mobiltelefonen an das WWW anzuschließen. „WAP“ steht für „Wireless Application Protocol“ und bezeichnet eine Infrastruktur von Gateways, die Mobiltelefone mit ihrer im heutigen GSM kleinen Bandbreite an das relativ aufwändigere HTML-Protokoll des World-Wide Web anschließen. Das WAP-Forum nennt WAP „the de facto worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants and other wireless terminals“ (WAP Forum 2000). Die Strategie, mobile Telefone in das Internet und in den elektronischen Geschäftsverkehr zu integrieren, hat uns ein neues Schlagwort beschert: „Mobile Commerce“ oder kurz „M-Commerce“.

Smartcards bilden eine Art Sicherheitsanker, die Menschen mit sich führen und die ihnen über personifizierte Verschlüsselungscodes sichere Zugänge ins Internet verschaffen. Darüber hinaus erlauben sie Zugang zum elektronischen „Point-of-Sale“, etwa mit der EC-Scheckkarte an der Tankstelle, oder über eine Geldkartenfunktion als elektronischer Geldbörse.

Die *elektronische Signatur* ist eine technische Basis dafür, unabstreitbare Versprechen und authentische Daten digital über offene Netze auszutauschen. Sie beruht auf moderner Kryptographie. Alle Teilnehmer verfügen über persönliche Verschlüsselungsparameter, sogenannte Schlüssel, mit Hilfe derer sie digitale Texte individuell und unnachahmlich verschlüsseln können. Das Kryptogramm ist die elektronische Signatur und wird mit dem Klartext gemeinsam weitergege-

ben. Eine Signatur wird verifiziert, indem sie „entschlüsselt“ und mit dem Klartext verglichen wird. Auf diese Weise wird festgestellt, dass nur der Inhaber des zugehörigen Schlüssels diesen Text so hat signieren können. Eine elektronische Signatur ist auch vom Signierer später nicht abstreitbar. Zu technischen Details s.z.B. Schneier (1996) oder Schmeh (1998).

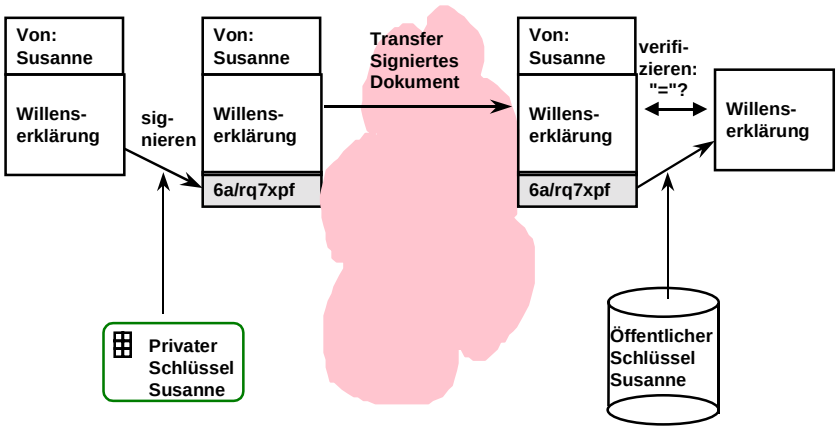

Abb. 1: Digitale Signatur

Schließlich bilden die zahlreichen jungen Entwicklungen zur *elektronischen Zahlung* einen wichtigen technischen Motor für E-Commerce. Wenn es misslingt, elektronisches Bezahlen selbstverständlich zu machen, wird es keinen E-Commerce geben. Welches der Systeme und Modelle sich durchsetzen wird, ist dagegen aus heutiger Sicht offen. Es gibt Protokolle zum Austausch von Zahlungsversprechen (SET, Kreditkarten) und andere zur Übermittlung digitalen Geldes (Ecash, Geldkarte). In wieder anderen Verfahren verwalten dritte Parteien Zahlungsbilanzen zwischen Käufer und Verkäufer (Paybox, Millicent, Cybercash). (BSI 1998, DUD 1999)

2. Das Vertrauensproblem

Die vorhandene Technik und ihre Entwicklungsperspektiven bilden ein dynamisches Potential zur Revolutionierung des traditionellen persönlichen und papierbasierten Handels. Allerdings geht nicht alles so einfach wie es aussieht. Offensichtlich wird heute über E-Commerce und M-Commerce mehr geredet als gehandelt. Die Fantasie ist groß, in der Wirklichkeit dagegen kommt E-Commerce nur schleppend voran. Das gilt insbesondere für das Privatkundengeschäft. Im Firmenkundengeschäft fällt es leichter, bilaterale Verabredungen zu treffen und die Kommunikation nach bestehenden Regeln einfach auf das Internet zu verlagern. Im Firmenkundengeschäft kennen sich die Geschäftspartner und brauchen sich ihre Regeln und Identitäten nicht erst zu beweisen. Im Privatkundengeschäft, jedenfalls im Massengeschäft, kennen sich die Partner dagegen nicht, hier müssen Regeln oft im Einzelfall erst verabredet werden. Im Privatkundengeschäft gibt es ein *Vertrauensproblem*, das auf Sicherheitsmängeln der technischen Basis, insbesondere des Internets, beruht.

Das Internet *verbindet* nämlich nicht nur Menschen, sondern es *trennt* sie auch. Die natürlichen Sinne stehen dem Menschen nicht mehr zur direkten Erkennung der Kommunikation zur Verfügung: Im Internet sieht, hört und fühlt man sich nicht. Die „Biologie“ der persönlichen Präsenz wird durch geschriebenen Text ersetzt, der nicht direkt dargestellt, sondern durch elektronische Geräte vermittelt wird. Um einen Text zu lesen, genügt es nicht mehr, das Blatt Papier vor Augen zu halten, das der schreibende Kommunikationspartner unter seinen Händen gehabt hat, sondern es sind Tastaturen, Leitungen, Bildschirme, Drucker und ihre Verarbeitungsprogramme vonnöten. Auf dem Weg von der Hand des Schreibers bis zum Auge des Lesers kann viel geschehen, um Text zu verstümmeln, zu löschen, oder gar komplett zu fälschen. Da man sich über das Internet nicht sicher erkennen kann, kann man hinterher leicht alles abstreiten, woran man sich nicht mehr halten will.

Im Internet fließt alle Kommunikation unverschlüsselt durch ein Netz von Subnetzen hindurch, auf deren Politik man nicht den geringsten Einfluss hat. Man weiß nicht, wer mit welchem Interesse mitliest, es gibt keine Vertraulichkeit. Daraus ergibt sich das Problem der Privatheit (englisch: „Privacy“): die Befürchtung vor dem gläsernen Internet-Kunden hält viele Menschen davon ab, im Internet aufzutreten. Ungefragte Massenreklame sind längst ein lästiges Alltagsproblem im Internet geworden, von der man nicht weiß, woher sie kommt, was ihre Produzenten noch alles von einem wissen und was sie mit diesem Wissen anstellen.

Außerdem ist das Internet unzuverlässig. Kommunikationsverbindungen brechen zusammen, Daten gehen verloren, Partner finden sich nicht wieder, und wenn doch, wissen sie nicht, wo sie aufgehört hatten. Ein Geschäft, das in der Luft hängen bleibt, ist schlechter als ein Geschäft, das man gar nicht erst angefangen hat.

3. Das Internet

Dem Internet fehlt es an einem überzeugenden Sicherheitskonzept. Es gibt keine Standardverfahren zur *Authentifizierung* von Personen, Prozessen oder Daten. Es gibt erst seit Neuerem Protokolle für das World-Wide Web, die in Einzelfällen (zum Beispiel bei Homebanking regelmäßig eingesetzt) eine verschlüsselte Kommunikation zwischen Browser und Server vorsehen (SSL 1996), aber andere Anwendungen wie E-Mail, File Transfer oder Chats und selbst die Übertragung von Passwörtern finden in der Regel *unverschlüsselt* statt. Es gibt keine Maßnahmen gegen den *Verlust von Daten*, gegen den *Ausfall von Diensten* und gegen das *Ausspionieren* von Datenkommunikation. Das Internet ist dazu zu einfach gebaut. Das ist kein Wunder, denn die Entstehungsgeschichte des Internet wäre eine andere, wenn man das Sicherheitsproblem in die Grundarchitektur aufgenommen hätte, so wie es die Ingenieure geschlossener, zentral kontrollierbarer Netze selbstverständlich immer vorsehen würden und vorgesehen haben. Aber das Internet ist ja kein geschlossenes Netz. Es ist nicht zentral kontrollierbar. Der ungeheure und historisch einmalige Erfolg des Internet beruht gerade darauf, dass es einfach ist, dass es offen ist und dass es niemandem gehört.

Es gibt eine reiche Literatur über die Technik des Internet. Zu den umfassenden Standardwerken gehört Comer (1988). Eine hübsche und sehr kurze Einführung in das Zusammenspiel der verschiedenen Komponenten, insbesondere über den Routing-Mechanismus, bieten Scolofsky und Kale (1991).

Das Internet ist ein weltweiter Verbund von lokalen Netzen, die völlig verschiedene lokale Techniken haben können. Eine der Grundideen des Internet besteht gerade darin, verschiedene lokale Netztechniken derart zu verknüpfen, dass sie in der globalen Kommunikation keine Rolle mehr

spielen. Mehr noch: Der Internet-Nutzer braucht überhaupt nicht mehr zu wissen, auf welcher lokalen Technik das Internet beruht. Ob nun Ethernet, Fast-Ethernet, Token Ring, Datex-P oder FDDI, sie können alle durch einfachste Erweiterung in den Datagramm-Verkehr des Internet einbezogen werden. Ja sogar die Telefonnetze mit ihren festen und mobilen Telefonanschlüssen sind längst Bestandteil des Internet.

Jedes lokale Netz muss nur folgende Fähigkeiten besitzen, damit es ans Internet angeschlossen werden kann: Seine lokalen Komponenten müssen über das globale Adressierungsschema des Internet von außen ansprechbar und ihrerseits in der Lage sein, globale Adressen außerhalb des eigenen lokalen Netzes anzusprechen (Scolofsky 1991). Die lokalen Netze verfügen an ihren externen Ein- und Ausgängen über Router, die entscheiden, wohin ein- und ausgehende Datenelemente zu senden sind („Routing“) und die die hereinkommenden Internet-Datagramme in lokale Datenelemente übersetzen und umgekehrt hinausgehenden lokale Datenelemente in globale Internet-Datagramme. Das regelt das Internet-Protokoll („IP“) und wird von den lokalen Modulen der ans Internet (bzw. an ein lokales Netz im Internet-Verbund) angeschlossenen Rechner realisiert. Alles andere ist Sache der lokalen Geräte und Programme innerhalb des Netzes.

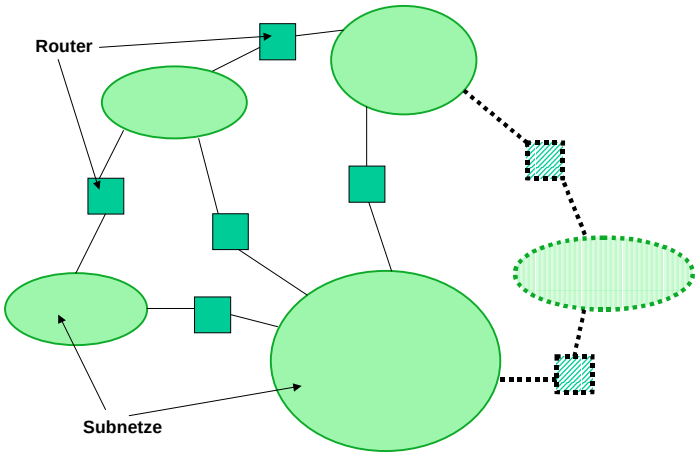

Abb. 2: Horizontales Wachstum: Hinzufügen neuer Subnetze ins Internet

In diesem Sinne ist das Internet „horizontal offen“: Irgend ein lokales Netz kann sich einfach dadurch an das Internet anschließen, dass es einen Router zwischen sich und einem bereits an das Internet angeschlossenen lokalen Netz platziert und alle Datagramme, die aus dem lokalen Netz hinausführen, an diesen Router schickt. Der Anschluss an das Internet ist also eine rein lokale Entscheidung zwischen zwei „befreundeten“ lokalen Netzen. In diesem Sinne gehört das Internet niemandem. Ob eigene Datagramme in ihrem Hopping durchs Internet über dieses oder jenes lokale Netz geroutet werden, liegt außerhalb der Entscheidung des Senders oder Empfängers. Ebenso ist nicht kontrollierbar, was alles mit einem Datagramm im Internet geschieht, insbesondere, wer alles mitliest.

Damit werden zwar Datagramme weltweit und technologieunabhängig verteilt, aber damit funktionieren noch keine Kommunikationsanwendungen wie E-Mail oder das World Wide Web. Diese benötigen weitergehende lokale Funktionen. Die lokalen Internet-Module sind so programmiert, dass sie alle Datagramme, die nicht für den eigenen Rechner bestimmt sind, ignorieren, während sie die Datagramme an die eigene IP-Adresse an die richtige Anwendung im eigenen Rechner weiterreichen. Zu diesem Zweck enthalten die hereinkommenden Transportnachrichten

sogenannte „Portnummern“ (die beim Absenden von der absendenden Anwendung eingetragen werden). Das Internet-Protokoll ignoriert beim Routen der Datagramme durch das Internet die Anwendungsbezüge. Salopp gesprochen: das Internet-Protokoll „kennt keine Anwendungen“.

In diesem Sinne ist das Internet „vertikal offen“: irgend eine neue Anwendung kann in das Internet eingeführt werden, ohne dass das bestehende Internet es überhaupt wahrnimmt, also auch ohne dass irgendeine existierende Anwendung davon gestört würde. Eine Anwendung wird in das Netz eingeführt, indem der Anwendungsprogrammierer die kommunizierenden Automaten implementiert und auf einem Teilnetz des Internet (im einfachsten Fall auf zwei durch das Internet verbundenen Rechnern) installiert. Die neuen Anwendungskomponenten würden dann ihre Anwendungsdaten innerhalb von Datagrammen über das Internet hinweg austauschen, wobei das Internet lediglich dafür sorgen wird, dass sie am richtigen Zielrechner ankommen. Dort würden die Internet-Module die eingehenden Pakete auf Grund der neuen Portnummern an die neu installierten Anwendungskomponenten weiterreichen und diese würden sie dann programmgemäß verarbeiten. Der einzige Haken ist, dass das Internet nichts für die Sicherheit der übertragenen Datenpakete tut. Das müssen die Anwendungskomponenten schon selbst tun.

Deshalb kann das Internet auch in seiner Anwendungsvielfalt ungebremst wachsen. Wir haben es zum Beispiel seit 1992 erlebt, dass sich das World Wide Web ungehindert (und ungeheuer rasch) global etablieren konnte, ohne dass die bestehenden Kommunikationsdienste des Electronic Mail und des Datentransfers im Mindesten gestört worden wären.

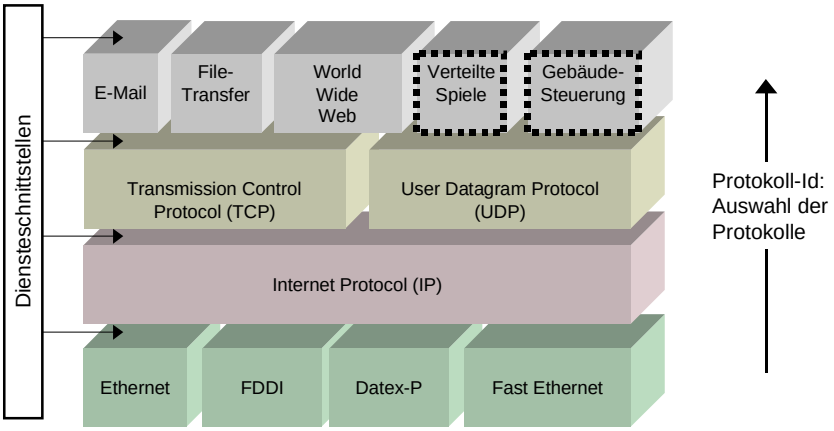

Abb. 3: Vertikales Wachstum: Hinzufügen neuer Anwendungen ins Internet

Aus dieser Grundarchitektur des Internet sind folgende Konsequenzen zu ziehen: Erstens, das Internet ist global unsicher, während es lokal sicher gemacht werden kann. Zweitens, Sicherungsdienste gehören in die Endanwendungen, und nicht in den Routingkern.

4. Die Lücke zwischen lokaler Sicherheit und globaler Unsicherheit

4.1 Die Lücke

Das Internet provoziert die Zukunftshoffnung global und unmittelbar wirkender elektronischer Kommunikation. Gleichzeitig ist das Internet unsicher, so dass man sich nicht darauf verlassen kann, dass alles so funktioniert, wie es soll. E-Commerce ist bis heute noch lange keine akzeptierte Realität. Handel, Geschäft und private Kommunikation brauchen Vertrauen. Worin besteht denn nun im Internet die Vertrauenslücke? Und welche Technik braucht das Internet zur Unterstützung vertrauenswürdiger Kommunikation zwischen Menschen?

Das Internet reicht zwar weltweit, aber es gibt keine globale Kontrolle über das Funktionieren des Internet. Das Internet gehört niemandem, es ist ein lose verbundenes Netz von Millionen von autonomen Teilnetzen. Es gibt keine zentralen Sicherungsverfahren. Kontrollen beschränken sich auf den lokalen eigenen Herrschaftsbereich, global herrscht in Bezug auf die Sicherheitspolitiken das unkontrollierte Chaos.

Man kann im Internet nicht sicher sein, dass die Kommunikationspartner wirklich die sind, die sie zu sein vorgeben. Man kann sich nicht darauf verlassen, dass Versprechen eingehalten und Verträge anerkannt werden. Man weiß nicht, ob die technischen Funktionen frei von Manipulationen sind, ob Dienstleistungsserver einwandfrei verfügbar sind und ob sie sich wohl verhalten. Man weiß auch nicht, wer alles mithört, ob sensible und wertvolle Informationen geschützt sind und ob alle Daten unverletzt übertragen und gespeichert werden. Kurz, von seiner technischen Grundausstattung her scheint das Internet noch weniger zu verbindlicher Geschäftskommunikation zu taugen als das Telefon.

Die Vertrauenslücke besteht zwischen der *Lokalität* der durchsetzbaren Sicherheit und der unkontrollierbaren *Globalität* der Kommunikationswirkung.

4.2 Ende-zu-Ende Sicherheit

Die Sicherheitsphilosophie des Internets besteht darin, dass das Netz in seinem “Inneren“, d.h. in Bezug auf das Routing von Datagrammen, unsicher ist, während zusätzliche Sicherungsdienste an seinen „Rändern“, d.h. in den Anwendungen, den Internetbetrieb nicht stören und auch dann funktionieren, wenn das Internet selbst unsicher ist. Die Infrastruktur zum globalen Routing von Datagrammen kann keine global zuverlässigen Sicherungsdienste wie Verschlüsselung, Authentifizierung und Qualitätsgarantie erbringen.

Sicherheit gibt es nur auf diesen beiden Ebenen:

Erstens innerhalb eines lokalen Netzes, das von einer verantwortlichen Stelle kontrolliert wird. Hier können Zugriffe geschützt, Datenfluss gefiltert, Identitäten überprüft, Qualität garantiert und Dienstleistungen integer und aktiv gehalten werden, indem die Netzkontrolle sich um jede einzelne Komponente kümmert und alle Teilnehmer die Maßnahmen der Netzkontrolle akzeptieren.

Zweitens können Sicherungen auf Anwendungsebene installiert werden, die auch über das unsichere Internet hinweg wirken. Beispiele dafür sind Verschlüsselung von Anwendungsdaten, Signierung von digitalen Dokumenten und das Vorhalten redundanter Dienste zum Ersatz für ggf. ausfallende Dienstleistungen. Alle Sicherungen, die von Anwendungsdiensten erbracht werden können, werden im Internet wie Anwendungen behandelt, d.h. sie leben friedlich neben den anderen Anwendungen und wirken unabhängig von der zu Grunde liegenden (unsicheren) Netztechnik.

4.3 Globale und lokale Bestandteile

Lokal sind Computer, ihre Software und Zugänge ins Internet. Lokal sind auch die Mensch-Maschine-Schnittstellen wie zum Beispiel die Ein- und Ausgabegeräte. Lokal sind Verhalten und Wahrnehmung der Menschen. Die Menschen agieren lokal in ihrem Kommunikationszugang.

Global hingegen ist das Netz mit seiner Kommunikationsreichweite. Und global sind die Ansprüche der Menschen, die soweit reichen wie ihre Kommunikation. Entsprechend gilt auch ihre Verantwortung global. Global sind die Regeln des Zusammenlebens, global sind die Wirkungen der Kommunikation wie Versprechen, Verpflichtungen, Verträge.

Global ist vor allem der E-Commerce. Dieser soll ja gerade nicht nur in kleinen geschlossenen Kreisen stattfinden, sondern auf einem offenen Markt, d.h. über die eigenen Organisationsgrenzen hinaus. Man sucht das Geschäft mit Partnern, die man nur eingeschränkt, vielleicht zunächst gar nicht kennt und denen man nur eingeschränkt traut. Man möchte sowohl langfristige Geschäftsbeziehungen aufbauen und pflegen können, als auch kurzfristige. In einigen Business-Modellen („Wochenmarkt“) trifft man sich vielleicht nur einmal im Netz, um ein Geschäft anzubahnen, vielleicht wieder abzubrechen oder doch zu Ende zu führen, um sich dann nie wieder zu sehen. Hier wird also nach einer global zuverlässigen E-Commerce-Infrastruktur gesucht. Wie kann die Lücke zwischen lokaler Sicherheit und globaler Unsicherheit geschlossen werden? Und in wieweit *soll* sie überhaupt geschlossen werden?

Die Lösung liegt im richtigen Zusammenspiel zwischen Menschen und Maschinen einerseits, und zwischen lokalen und globalen Mechanismen andererseits. Die Verbindung zwischen der lokalen Sicherheit und der globalen Unsicherheit wird auf zweierlei Wegen hergestellt: erstens durch ein *global gültiges Regelwerk*, d.h. durch ein anerkanntes *Rechtssystem*; zweitens durch die Koordination lokaler Verhaltensweisen nach den globalen Regeln, d.h. durch *globale Infrastrukturen* lokaler Vertrauensdienste.

Beweise verknüpfen lokales Verhalten mit globalem Recht. Beweise fallen *lokal* an, sie sind *lokal* schützbar und prüfbar, aber ihre Wirkung wird *global anerkannt*. Die aufzubauenden Infrastrukturen müssen demnach in der Lage sein, lokal Beweismittel zur Verfügung zu stellen, die global anerkannt werden. Den State-of-the-Art bilden heute elektronische Signaturen auf der Basis mathematischer kryptographischer Verfahren.

Statt einer global beherrschten Technik, wie man sie etwa noch aus den Zeiten der nationalen Telekom-Monopole kannte, müssen nun autonome Dienstleistungen nach verabredeten technischen Standards und nach verabredeten globalen Rechtsregeln miteinander kooperieren.

4.4 Forschungsaufgaben

Damit stellt der Aufbau vertrauenswürdiger Kommunikation im Internet die folgenden vordringlichen Forschungsaufgaben:

1. *Signaturen:* die Entwicklung von elektronischen Signaturverfahren, ihre Unterstützung durch Trust-Infrastrukturen in Form von Zertifizierungs- und Notariatsdiensten, sowie ihre Einbindung in elektronische Geschäftsvorgänge.
2. *Standardisierung*: die Standardisierung von Kommunikationsregeln und ihren Sicherungsfunktionen.
3. *Recht*: die Entwicklung technikadäquater rechtlicher Systeme.

4. *Beweise*: die Entwicklung von Mensch-Maschine-Schnittstellen, die das richtige Zusammenspiel von Verpflichtungen und Beweisen lokal nachvollziehbar durchsetzen.
5. *Personalisierung und Privatheit*: die technische Unterstützung für Dienste, die auf individuelle persönliche Bedürfnisse der Anwender zugeschnitten sind, bei gleichzeitigem Schutz der Privatsphäre. Die Respektierung der Privatheit ist eine zentrale Voraussetzung für Vertrauen.
6. *Komplexe Anwendungen:* die Integration mehrerer Anwendungen in größere inhaltliche Zusammenhänge; Beispiele: die Integration von Vertragsabschlüssen und Zahlungsverfahren in Geschäftskooperationen; das richtige Zusammenspiel von Anonymität und Identifizierung in Internet-Wahlen; die Entwicklung von Tele-Diensten, z.B. Tele-Universitäten.
7. *Automat und Mensch*, Intention und Interpretation: ein Verständnis der Grenze zwischen Automat und Mensch, so dass die Menschen ihre Absichten in Bezug auf die wertvollen Kommunikationsinhalte mit Hilfe der Kommunikationstechnologie adäquat zum Ausdruck bringen können.

Erst in einem Kontext dieser Lösungen werden Kooperationssysteme die notwendige Akzeptanz finden, die der E-Commerce bei aller Zukunftshoffnung noch bei weitem nicht hat.

Teil 2: Wie sicher soll E-Commerce sein?

Im folgenden zweiten Teil dieses Artikels soll der letzte Punkt 7, die Forschungsaufgabe „Automat und Mensch“ genauer beleuchtet werden.

5. Automat und Mensch – Intention und Interpretation

Menschen kommunizieren, indem sie Daten austauschen, die sie mit inhaltlichen Werten belegen. Sie entnehmen den hereinkommenden Daten einen inhaltlichen Wert, indem sie sie interpretieren. Sie legen umgekehrt ihre inhaltliche Absicht in den Ausdruck der hinausgehenden Daten. Die Frage ist: wieviel kann der Automatismus einer Kommunikationstechnologie leisten, um den Menschen in seinen inhaltlichen Interpretationen und Absichten maximal zu unterstützen und zu entlasten, ohne die Kommunikation zu verfälschen. Wenn man den Automaten zu viel zumutet, d.h. wenn die Automaten nicht mehr in der Lage sind, die ursprüngliche Intention einer Kommunikation auszudrücken, dann kommt es zu Missverständnissen, die schlimmstenfalls sogar in böser Absicht ausgenutzt werden können. Dann werden die Menschen die Technik nicht mehr nutzen. Mutet man den Automaten dagegen zu wenig zu, bleiben Potenziale zur Entlastung und zur Kostenersparnis ungenutzt.

Ein Beispiel für dieses Dilemma auf einem anderen technologischen Gebiet bilden die Start- und Landefunktionen von Verkehrsflugzeugen. Bei aller Automatisierung, die die Arbeit der Piloten vereinfacht und dadurch Starten und Landen gleichmäßiger, glatter und sicherer macht, müssen die Piloten dennoch jederzeit in der Lage sein, manuell einzugreifen, um nicht vorhergesehene Situationen abfangen zu können. Einem unfallträchtigen Roboterpiloten, der zu simpel gestrickt ist, werden sich keine Passagiere mehr anvertrauen wollen. Die Mannigfaltigkeit der Start- und Landesituationen ist derart komplex, dass kein Roboter der Welt sie in jedem Fall aufgrund vordefinierter Spezifikationen bewältigen kann. Das gilt noch viel mehr für die Kommunikationstechnik.

6. Vertrauen

Die Frage, wo die Grenze für eine technische Unterstützung menschlicher Kommunikation im E-Commerce liegt, hängt eng mit der Frage zusammen, worauf das *Vertrauen* beruht, dass ein Mensch in die verwendete Kommunikationstechnik haben muss. Das soll in diesem Abschnitt besprochen werden. Das Internet wird allgemein als wenig vertrauenswürdig bezeichnet, da es zu unsicher sei. Wieviel Sicherheit aber soll das Internet überhaupt bieten, damit es vertrauenswürdigen E-Commerce erlaubt?

Vertrauen ist die Gewissheit (d.h. eine innere Repräsentanz des Eintretens) einer erwünschten Zukunft. Es beruht

- auf der Kontinuität des regelhaften und erwünschten Verhaltens der Umgebung
- oder auf der Hilfe vertrauter Menschen (auch in unwägbarer Lage)
- oder auf der eigenen Kenntnis und Beherrschung der Lage (einschließlich ihrer Unwägbarkeiten)

Diese drei Elemente von Vertrauen schließen sich nicht aus, im Gegenteil: sie ergänzen sich in aller Regel. Misstrauen übrigens, um das Bild zu vervollständigen, entsteht als Komplement zum Vertrauen entweder aus einer Ungewissheit über die Zukunft *oder* aus der Gewissheit des Eintretens einer unerwünschten Zukunft. Misstrauen beruht also auf:

- Diskontinuität akzeptierten oder abgelehnten Verhaltens: „man kann sich nicht darauf einstellen“, „das ist nicht steuerbar“, „nicht vorhersehbar“;
- oder Kontinuität abgelehnten Verhaltens: „der hat schon immer gelogen“;
- und Hilflosigkeit: „wenn etwas schief geht, hilft mir keiner“.

Der erste Punkt in der Definition von Vertrauen, „Kontinuität des regelhaften Verhaltens der Umgebung“ beruht auf der Funktionalität der Umgebung. In einer technischen Umgebung, wie etwa den Kommunikationsmedien von E-Commerce, wird das regelhafte Verhalten durch technische und organisatorische Verfahren erreicht. Die beiden anderen Punkte, „Hilfe durch andere Menschen oder durch eigene Kraft“, beziehen sich auf Menschen.

Es ist die Frage, wie weit die Grenze zwischen Mensch und Technik in Richtung Technik verschoben und dabei das Vertrauen in das regelhafte und erwünschte Verhalten der technischen Umgebung erhöht werden kann. Wie viele Anteile, die bisher von Menschen ausgeübt werden müssen, können spezifiziert und den Funktionen eines Automaten übertragen werden? Wird Vertrauen dadurch erhöht, dass schließlich alle Funktionen auf die Technik übertragen werden, oder ist die Möglichkeit zum menschlichen Eingriff eine notwendiger Voraussetzung dafür, dass man einer Sache vertraut?

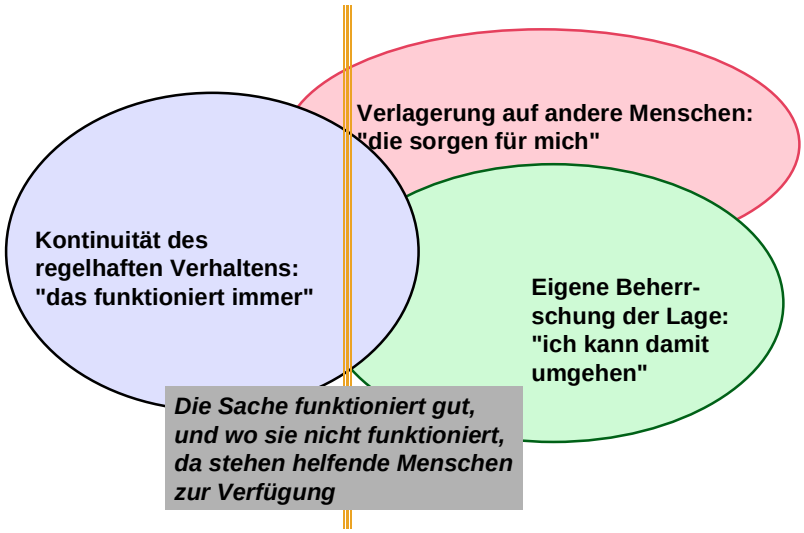

Abb. 4: Grenze zwischen Mensch und (technischer) Funktionalität bei „Vertrauen“

Im obigen Beispiel des Autopiloten wird die Handsteuerung bei Start und Landung eines Flugzeugs einem Automaten übertragen, der die Umwelteinflüsse kontinuierlich auswertet und das Flugzeug entsprechend steuert. Im Beispiel der Kommunikationstechnik können zum Beispiel Suchfunktionen, Verbindungsaufbau und das Makeln zwischen verschiedenen Verbindungen automatisiert werden. Weitergehend sind auch standardisierte Auskünfte automatisierbar, wie das bereits heute viele Telefondienste, zum Beispiel beim Telefonbanking anbieten. Noch weitergehend könnte ein persönlicher Softweareagent Entscheidungen treffen, die sich aus der Kommunikation ergeben, beispielsweise automatische An- und Verkäufe von Aktien aufgrund von Börseninformationen.

Die Frage nach der Automatisierung menschlicher Handlung kann man sich auch für die Sicherheit stellen. Wie viel automatische Sicherheit kann Kommunikationsrisiken von vorne herein ausschalten und wie viel Risiko soll bei den handelnden Menschen verbleiben?

7. Wittgensteins Sprachspiele

Ludwig Wittgenstein hat in seinem Tractatus logico-philosophicus (1922) die These ausgeführt, das Ziel von Philosophie bestehe darin, eine vollständige und eindeutige sprachliche Analyse der logischen Zusammenhänge der Welt zu entwickeln.

Die Eingangssätze des Tractatus, „Die Welt ist alles, was der Fall ist“ (1) und „Die Welt ist die Gesamtheit der Tatsachen, nicht der Dinge“ (1.1) zielen auf eine logische Welt, deren wesentlichen Gehalt nicht die darin vorhandenen Elemente, sonder ihre Bezüge zueinander ausmachen. Der Anspruch des Tractatus liegt darin, die Welt vollständig und eindeutig zu beschreiben.

Die Vollständigkeit wird in dem Wort „alles“ zum Ausdruck gebracht („Die Welt ist *alles*, was der Fall ist“), sowie in zahlreichen anderen Äußerungen des Tractatus, zum Beispiel „Die Tatsachen im logischen Raum sind die Welt“ (1.13), „Die Welt zerfällt in Tatsachen“ (1.2) oder auch

„Der Satz kann die *gesamte* Wirklichkeit darstellen“ (4.12). Die Eindeutigkeit der Beschreibung fordert er zum Beispiel mit den Sätzen „Es gibt eine und nur eine vollständige Analyse des Satzes“ (3.25) oder „Alles, was sich aussprechen lässt, lässt sich klar aussprechen“ (4.116). Durch eine korrekte Analyse der Welt, so das Fazit des Tractatus, wird die Welt vollständig und abschließend erfasst, jedenfalls soweit Wissenschaft und Philosophie reichen können: „Wovon man nicht sprechen kann, darüber muss man schweigen“ (7), wie es in dem berühmten, wohlklingenden aber doch etwas mystischen Schlusssatz des Tractatus heißt.

In die moderne Welt der Computer übersetzt, könnte man die Forderung des Tractatus dahingehend erweitern, dass alles wesentliche menschliche Handeln in dieser Welt implementiert und durch Computer ausgeführt werden kann, wenn man es nur richtig anpackt. Die Forschungsaufgabe müsste demnach lauten, alle Handlungssituationen zu analysieren mit dem Ziel sie zu programmieren. Im Ergebnis würde jede analysierte Handlungssituation von einem Automaten ausgeführt und der Mensch davon vollkommen entlastet sein.

Dieser Vorstellung von der Welt lag die Hoffnung seiner Zeit der 1920er Jahre zu Grunde, dass die Mathematik diese Aufgabe wenigstens in ihrem eigenen Feld bewältigen könne. Die Mathematik galt (und gilt bis heute!) als das große Vorbild für alle wissenschaftliche Sprachen. Man konstruierte damals als Teil des Hilbertschen Programms zur Lösung bisher ungelöster großer mathematischer Probleme ein widerspruchsfreies Axiomensystem, mit dessen Hilfe die Mathematik der Zahlen und Geometrie eindeutig und vollständig erfasst werden könnte. Dass dieses Vorhaben schon für die (relativ) einfache Welt der Arithmetik der natürlichen Zahlen undurchführbar ist, und erst recht für die gesamte Mathematik, wusste man 1922 zur Zeit der Entstehung des Tractatus noch nicht. Die ersten früh erkannten Paradoxa (z.B. das „Russelsche Paradoxon“) in der Mengenlehre wurden irgendwie geflickt. Schließlich zerstörte Kurt Gödel (1931) die Hoffnung, dass es möglich sei, die Arithmetik mit einem formalen System sowohl vollständig und abschließend, als auch widerspruchsfrei zu beschreiben. Er bewies, dass ein formales, widerspruchsfreies logisches System von Sätzen für die Artihmentik unweigerlich Sätze enthält, die mit diesem System weder beweisbar, noch widerlegbar sind. Eine hübsche Beschreibung dieser Entwicklung findet sich etwa bei Hofstadter (1999).

Wittgenstein nahm an dieser Entwicklung aktiv teil. Der Schock durch die Erkenntnis von Gödel brachte ihn dazu, seinen Anspruch zur vollständigen Spezifizierung wissenschaftlicher Erkenntnis (und erst Recht menschlichen Handelns) aufzugeben. In seinem Nachlass finden sich Aufzeichnungen, die als Philosophische Untersuchungen (1953) veröffentlicht wurden, in denen er sich vom Tractatus abwendet und ein vollständig neues Modell der Sprache entwirft. Dieses Modell orientiert sich am Konzept des Spiels: „Ich werde auch das Ganze: der Sprache und der Tätigkeiten, mit denen sie verwoben ist, das ‚Sprachspiel‘ nennen“ (Philosophische Untersuchungen, 7). Wittgensteins „Sprachspiele“ haben großen Einfluss auf die moderne Sprachphilosophie. Die sogenannten Intentionalisten (etwa Searle 1980 und 1989) beziehen sich ausdrücklich auf das Modell der Sprachspiele. Von ihren „Sprechakten“ hoffen wiederum die Informatiker zu lernen, wie man die Mensch-Maschine-Schnittstelle für Kommunikationsautomaten richtig gestaltet.

In seinen Philosophischen Untersuchungen (1953) geht Wittgenstein davon aus, dass Sprache weder eindeutig noch vollständig ist. Sie ist jeweils kontextabhängig: „Die Bedeutung eines Wortes ist sein Gebrauch in der Sprache“ (43). Dabei folgt die Sprache in ihrem jeweiligen Kontext Regeln, die außerhalb des Kontextes stehen. Wie radikal er sich dabei von seinem Tractatus abwendet, macht etwa seine Aussage über die Ungenauigkeit deutlich: „Wenn ich einem sage ‚Halte dich ungefähr hier auf!‘ - kann denn diese Erklärung nicht vollkommen funktionieren? Und kann jede andere nicht auch versagen? [...] Verstehen wir aber nur, was ‚unexakt‘ bedeutet!

Denn es bedeutet nicht ‚unbrauchbar‘“ (88). Er erhebt hier offenbar nicht den Anspruch, das Phänomen der Sprache abschließend verstanden zu haben (wie noch zu Zeiten seines Tractatus).

Die Semantik eines Satzes ist nach diesem Verständnis nicht mehr durch die Syntax des Satzes vollständig gegeben. Die Semantik hängt von den Regeln des jeweiligen Sprachspiels ab, und die sind nicht in dem Sprachspiel selbst formuliert. Das ist wie bei einem richtigen Spiel: Bevor man es beginnt, muss man die Regeln kennen. Und wie lernt man die Regeln eines Sprachspiels? Nun, das ist ein anderes Sprachspiel. Demnach sind Sprache, wissenschaftliche Erkenntnis und letztlich menschliches Handeln offene Prozesse.

Was muss denn nun zur Syntax eines Satzes hinzukommen, um seine Semantik zu bestimmen? Searle (1989) fügt zur Syntax eines Satzes einen (nicht notwendig spezifizierten oder gar spezifizierbaren) „Hintergrund“ hinzu, mit dem gemeinsam die Semantik und ihre praktische Bedeutung eines Satzes bestimmt wird. Ein Satz („Sentence“, „Syntax“, „Daten“) ergibt erst im Kontext eines „Hintergrunds“ („Background“, „Kompetenz“, „Spiel“) die anwendungsorientierte Bedeutung („Application“, „Semantik“, „Information“). Informatiker würden eher von „Daten und Information“ als von „Syntax und Semantik“ sprechen.

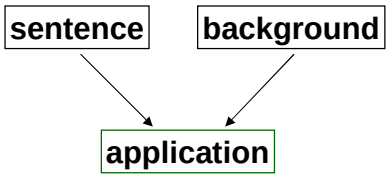

Abb. 5: Syntax und Hintergrund bestimmen die Semantik eines Satzes

Auf unsere Fragestellung angewendet: Menschen sind nicht vollständig automatisierbar. Die Kommunikationstechnik kann nicht zur Aufgabe haben, menschliches Handeln vollständig zu implementieren. Kommunikationssysteme enthalten Schnittstellen, an denen die kommunizierenden Menschen ihre Absichten und Interpretationen zur Geltung bringen können. Eine wesentliche Eigenschaft von kommerziellem Handel (wie von jeder wertvollen Kommunikation) besteht darin, dass Menschen zwar *miteinander* kommunizieren (reden, handeln, verabreden), dabei aber *unterschiedliche,* ja *gegensätzliche* Interessen vertreten können. Das Modell des Spiels macht es deutlich: Im Spiel spielen die Menschen sowohl *miteinander* nach gemeinsamen Regeln, als auch *gegeneinander* auf Sieg und Niederlage. Das Spielmodell taugt auch für den Geschäftsverkehr: Käufer und Verkäufer handeln gemeinsam Ware gegen Geld und wahren dabei ihre individuellen Interessen.

Die Aufgabe für die Entwicklung von E-Commerce-Systemen und ihren Sicherheitsfunktionen besteht also nicht darin, durch hundertprozentige Sicherheit alle Risiken auszuschalten, sondern die formalen Risiken auf Bruch der Geschäftsregeln zu beseitigen, damit sich die Menschen auf die inhaltlichen Risiken des Geschäftes mit Hilfe der neuen Medien („E-Commerce“) einlassen können. Zur Formulierung dieser Aufgabe taugt ein Telekooperationsmodell, in dem Personen in formale Rollen eintreten und darin als Akteure formale Ziele verfolgen, mit denen sie als Personen inhaltliche Zwecke verbinden. Ich skizziere das Modell im Folgenden. Für eine ausführliche Darstellung einschließlich der Gleichgewichtsbedingung für Verpflichtungen und Beweise vgl.

Grimm (1994), für eine formale Darstellung vgl. Grimm und Ochsenschläger (2000). Eine lesbare Übersicht über Sicherheitsmodelle der Informatik findet sich bei Kessler und Mund (1993).

8. Ein Personen-Rollen-Akteure-Modell für Telekooperation

8.1 In Rollen handelnde Personen

Menschen streben Ziele an, mit denen sie einen Sinn, d.h. bestimmte Zwecke verbinden. Beispiel: Ein Kunde eines Autohauses schließt einen Kaufvertrag mit dem Autohaus (Ziel), um ein gutes Auto zu erwerben und dabei möglichst wenig Geld auszugeben (Zweck). Das Autohaus schließt denselben Vertrag mit dem Kunden (Ziel), um möglichst viel Geld dabei zu verdienen (Zweck). Man sieht hier schon: es gibt ein gemeinsames Ziel (den Kaufvertrag), aber unter Umständen verschiedene, ja sogar entgegengesetzte und auch nicht weiter ausgeführte Zwecke.

Das ist ein wesentliches Merkmal des Telekooperationsmodells: Das Ziel ist grundsätzlich explizit und gemeinsam. Der Sinn des Ziels (der „Zweck“ der Kooperation) ist nicht explizit und nicht notwendig für jeden Teilnehmer derselbe. Hier sind Konflikte möglich, und genau diese Situation soll kooperationstechnisch auch unterstützt werden.

Um ihre Ziele zu erreichen, befolgen Menschen Handlungsmuster, die nach ihrer Erfahrung gute Aussichten auf Erfolg bieten. Im Kontext des Telekooperationsmodells bezieht sich das Wort Ziel auf den Endpunkt eines Handlungsmusters und das Wort Zweck auf den Sinn, den ein Mensch mit dem Erreichen des Handlungsziels verbindet.

Handlungsmuster werden als Rollen modelliert. Rollen sind spezifizierte Handlungsanweisungen (Skripte, Programme), die nicht-deterministische Verzweigungspunkte enthalten, in denen eine Person, die in einer Rolle aktiv ist, zwischen vorgegebenen Handlungsalternativen aufgrund persönlicher Kompetenz wählen kann. An anderen nicht-deterministischen Verzweigungspunkten beeinflusst nicht die Person, sondern die Außenwelt die Wahl zwischen den vorgegebenen Handlungsalternativen. Eine Rolle ist durch das Handlungsmuster sowie eine Menge von Kompetenzattributen definiert. Das Handlungsmuster enthält wohldefinierte Ein- und Austrittspunkte und möglicherweise nicht-deterministische Verzweigungspunkte. Die Spezifikation einer Rolle assoziiert mit einer wohldefinierten Teilmenge von Austrittspunkten das erfolgreiche Handlungsziel. Eine Person muss im Besitz der in einer Rolle spezifizierten Kompetenzattribute sein, um in dieser Rolle aktiv sein zu können.

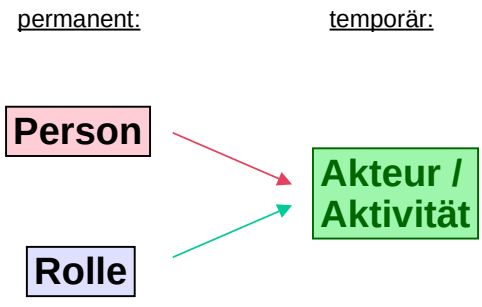

Abb. 6: Person tritt in Rolle ein und wird dadurch zu einem temporären Akteur

Die Idee des Telekooperationsmodells besteht darin, eine Aktivität in einen spezifizierten Anteil und einen nicht-spezifizierten Anteil zu zerlegen. Der spezifizierte Anteil einer Aktivität wird in der Rolle untergebracht, und der nicht-spezifizierte Anteil einer Aktivität wird der Person zugewiesen. Die Rolle ist der Kandidat für das zu implementierende Programm, die Person der Benutzer des Programms.

Ein Akteur ist eine Person in einer Rolle. Eine Rolle ist nichts Aktives, sie ist ein spezifiziertes Handlungsmuster. Aktiv sind Personen und, indem sie temporär in Rollen agieren, Akteure. Rollen und Personen sind verschiedene Beschreibungsbestandteile eines Akteurs: die Rolle stellt dabei den geregelten Anteil dar, dessen zielorientiertes Handlungsmuster bis auf nichtdeterministische Verzweigungspunkte voll spezifiziert ist; und die Person stellt den nichtspezifizierten Anteil dar, der über die nicht-spezifizierte persönliche Kompetenz verfügt, Entscheidungen zu treffen.

Die Semantik einer Aktivität ist mit der persönlichen Kompetenz verbunden. Der Sinn einer Entscheidung, der Zweck einer Handlung, erschließt sich der Person, während in der Rolle nur das formale (syntaktische) Handlungsziel spezifiziert ist. Eine Person steuert eine Aktivität, indem sie an den Entscheidungspunkten die Ergebnisse des bisherigen Aktivitätsverlaufs zur Kenntnis nimmt, sie inhaltlich auswertet und dann je nach dem Sinn, den sie mit der ganzen Aktivität und ihrem angestrebten Ziel verbindet, so oder so entscheidet.

Es ist wie ein Spiel: Die Spielregeln liegen fest, und das Ende eines Spiels (sein syntaktisches Ziel) ist wohldefiniert. Aber an gewissen, ausdrücklich dafür vorgesehenen Punkten während des Spiels entscheidet der Spieler, wie er weiterspielt, und manche Spieler gewinnen und andere verlieren. Das Rollenmodell ist vom Sprachspielmodell Wittgensteins inspiriert.

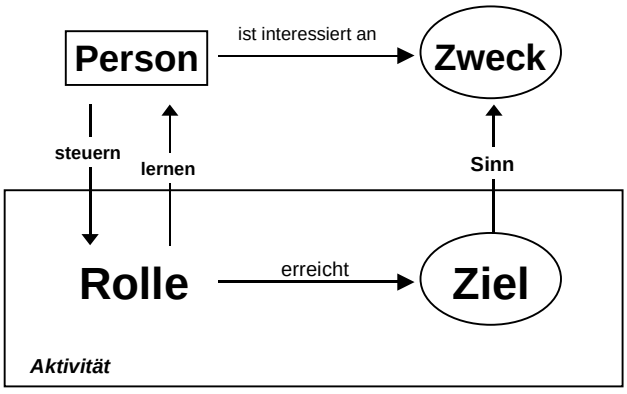

Abb. 7: Wechselbeziehung zwischen formalem Rollenziel und inhaltlichem Handlungszweck

Im E-Commerce sind kommunikative Handlungen von besonderem Interesse, also solche komplexe Situationen, in denen die Handlungen zweier (oder mehrerer) Personen sich aufeinander beziehen und gegenseitig beeinflussen. Dabei ist der Begriff eines *gemeinsamen Kooperationsziels* wichtig. Die Kooperationsrollen definieren ein allen gemeinsames Kooperationsziel, z.B. den Austausch eines Vertrags oder das Erreichen eines Zustandes, der übereinstimmend als regelgerechtes Spielende verstanden wird. Dagegen können die kooperierenden Personen durchaus verschiedene, ja gegensätzliche Zwecke mit demselben Ziel verbinden, z.B. Vor- und Nachteil

aus einem Vertrag, oder Sieg und Niederlage in einem Spiel. Während also die Akteure aufgrund wohldefinierter Protokolle ein gemeinsames Kooperationsziel anstreben, können die Personen damit unterschiedliche und sogar gegensätzliche Interessen verfolgen.

Es ist die Aufgabe von Kooperationstechnik, geeignete Rollen zu implementieren und auf diese Weise automatische Akteure zur Verfügung zu stellen, die die in den zugehörigen Rollen handelnden Personen vertreten. E-Mail User Agents und Web-Browser sind Beispiele für automatische Akteure. Für E-Commerce werden komplexe Akteure für Käufer- und Verkäufer gebraucht, die Verpflichtungssituationen verwalten und Zahlungs- und Warenlieferungsfunktionen integrieren. Ansätze dazu bieten elektronische Geldbörsen („Wallets“) und Zahlungsserver für elektronische Zahlungssysteme (BSI 1998, DUD 1999).

8.2 Akteur und Außenwelt

Die permanent vorhandene Person und die permanent vorhandene Rolle verschmelzen für eine temporäre Aktivität zu einem temporären Akteur. Die Permanenz ist hier auf den Lebenszeitraum der Person in einer Kooperationswelt bezogen: Die Lebenszeit einer Person in einer Kooperationswelt dauert so lange, wie sie in diesem Kontext handlungsfähig ist, und überdauert die Lebenszeiten ihrer Aktivitäten. Akteur und Aktivität sind verschiedene Aspekte desselben temporären Rollenspiels: Der Akteur repräsentiert die in der Rolle handelnde Person, die Aktivität bezeichnet den Ablauf der vom Akteur ausgeführten Aktionen. Als Akteur handelt die Person nach den Regeln der Rolle. Zur Entscheidung zwischen den in einer Rolle enthaltenen Handlungsalternativen bedarf es entweder eines Einflusses von außen oder der Kompetenz der in der Rolle handelnden Person, die sie beim Eintritt in die Rolle mit einbringt. Das bedeutet wegen des externen Einflusses, dass dieselbe Person, die dieselbe Rolle in verschiedenen Kontexten spielt, zu verschiedenen Handlungen und Ergebnissen kommen kann. Das bedeutet wegen der persönlichen Kompetenz weiterhin, dass zwei verschiedene Personen, die (unabhängig voneinander) dieselbe Rolle spielen, zu verschiedenen Handlungen und Ergebnissen kommen können.

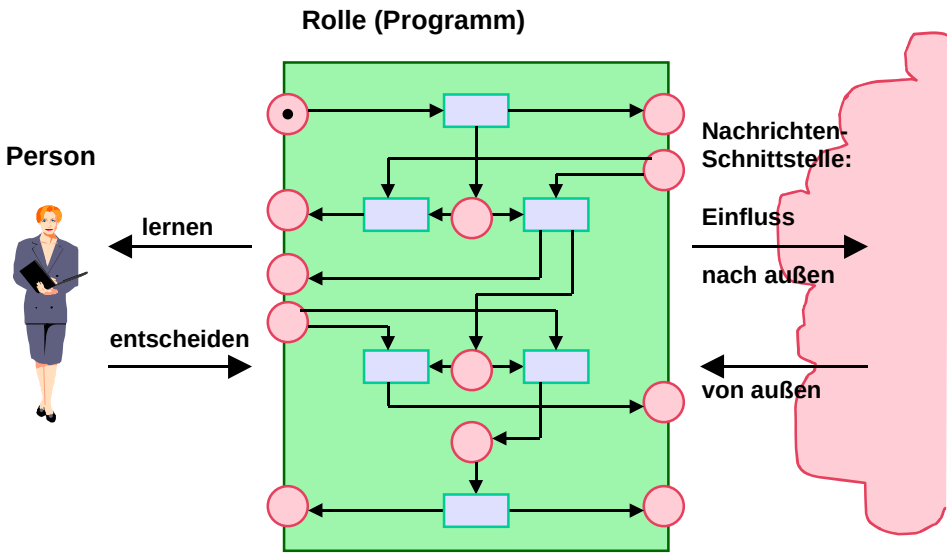

Abb. 8: Wechselbeziehungen Akteur – Außenwelt

Mit Hilfe ihrer Kompetenz greift eine Person an dafür vorgesehenen Punkten entscheidend in den Rollenablauf ein (kompetente Entscheidungen). Umgekehrt kann das Agieren in einer Rolle die Kompetenz der Person verändern (Lerninhalte). Lernen und Formulieren von Entscheidungen beruhen auf der Sprachkompetenz, die eine Person in die Aktivität mit einbringt. Im Laufe und nach Beendigung der Aktivität wertet die handelnde Person die empfangenen Nachrichten inhaltlich aus und verändert damit ihre Kompetenz. Personen mit ihren Kompetenzen sind beständige Elemente einer Rollenwelt, die einzelne Aktivitäten überdauern und mehreren Aktivitäten einen zusammenhängenden Sinn und eine zusammenhängende Struktur verleihen können. Ihnen wird daher auch „Permanenz“ zugeschrieben. Allerdings können auch neue Personen in eine Kooperationswelt eintreten, bzw. existierende Personen aus einer Kooperationswelt ausscheiden.

Die Wechselbeziehung zwischen einer Person und ihrer Außenwelt ist ausschließlich über den Akteur vermittelt: Der Akteur ist die Außenansicht einer handelnden Person, die der Außenwelt in einem bestimmten Kooperationskontext vermittelt wird. Korrespondierend dazu stellt der Akteur gegenüber der Person die der Person vermittelte Innensicht der Außenwelt dar. Diese Wechselwirkung wird über eine Nachrichtenschnittstelle zwischen dem Akteur und der Außenwelt modelliert: Die Einflüsse von außen auf den Akteur werden über Nachrichten aus der Außenwelt an den Akteur, die Einwirkungen des Akteurs auf die Außenwelt über Nachrichten vom Akteur an die Außenwelt ausgeübt.

Im Falle einer Kooperation zwischen zwei oder mehr Partnern sehen sich die Personen nur über ihre Außenbilder, das sind sie als Akteure. Sie kommunizieren nur als Akteure miteinander, und zwar über ihre jeweiligen Nachrichten-Schnittstellen zur Außenwelt.

8.3 Hierarchie von Akteuren

Es ist möglich, Entscheidungen, die eine Person bisher ohne automatische Unterstützung getroffen hat, zu programmieren und an einen Teilakteur zu delegieren. Zwei Akteure stehen in einem hierarchischen Verhältnis zueinander, wenn aus Sicht des untergeordneten Akteurs der übergeordnete Akteur die verantwortliche Person darstellt, indem dieser nämlich an den Verzweigungspunkten die Entscheidungen trifft. In der umgekehrten Richtung betrachtet: Der untergeordnete Akteur erfüllt eine Teilaufgabe des übergeordneten Akteurs. Das Ziel der untergeordneten Aktivität ist ein Teilziel der übergeordneten Aktivität. Der Zweck des Teilziels ist durch seine Einbettung in die übergeordnete Aktivität definiert.

Von oben nach unten betrachtet, beschreibt diese Hierarchie von Akteuren die Delegation von Aufgaben. Der übergeordnete Akteur stößt nämlich die untergeordnete Aktivität an und führt sie nach den Regeln der zugehörigen Rolle aus. Von unten nach oben betrachtet, beschreibt diese Hierarchie die Erweiterung von Spezifikationen. Der übergeordnete Akteur entscheidet nämlich zwischen den Alternativen, die in der Rolle des untergeordneten Akteurs spezifiziert sind, auf eine Weise, die aus Sicht des untergeordneten Akteurs nicht vorhersehbar ist. Aus Sicht des untergeordneten Akteurs sind solche Entscheidungen nicht spezifiziert, sondern in die Kompetenz der verantwortlichen Person gelegt. Im Rahmen der Rolle des übergeordneten Akteurs ist die Entscheidung aber gerade spezifiziert. Wenn also eine bisher nicht spezifizierte Entscheidung aufgrund neuer Kenntnisse oder durch Abgrenzung des Anwendungsumfeldes in einer neuen Rolle spezifiziert wird, dann wird die verantwortliche Person in dieser Entscheidung unterstützt, indem er hier von einem neuen Akteur, der dem bisherigen Akteur übergeordnet ist, vertreten wird.

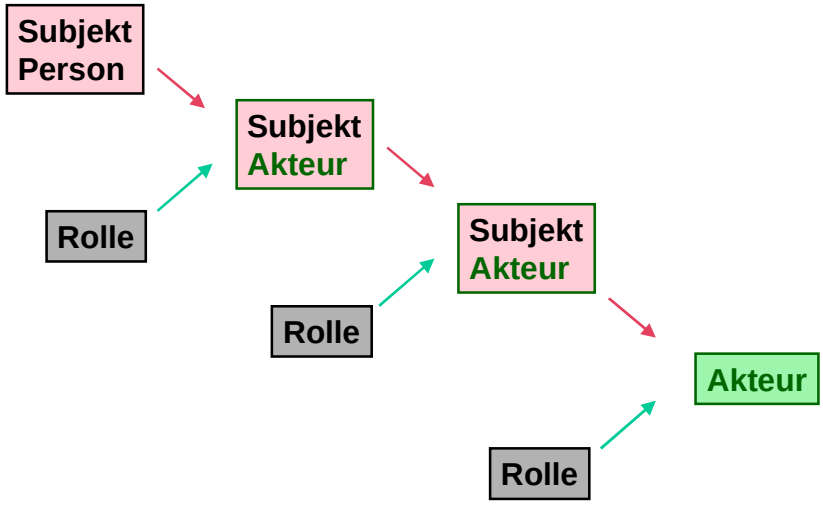

Abb. 9: Hierarchie von Akteuren

Ein übergeordneter Akteur repräsentiert gegenüber allen ihm untergeordneten Akteuren die verantwortliche Person. Er muss auch die akteursspezifische Kompetenz dem untergeordneten Akteur überreichen. Hinter dem obersten Akteur in einer solchen Hierarchie steht immer eine reale Person, die verantwortlich für alle ihre Akteure und Unterakteure ist. Ein Beispiel für derart hierarchisierte Aktivitäten ist die Abwicklung eines Zahlungsvorgangs (untergeordneter Akteur), im Auftrag eines Käufers bzw. Verkäufers (übergeordneter Akteur) im Rahmen eines Warenkaufs.

8.4 Kooperation zwischen Akteuren und Erfolgskopplung

Zwei oder mehr Akteure kooperieren, wenn sie über ihre Schnittstellen zur Außenwelt untereinander Nachrichten austauschen und wenn die zugehörigen Kooperationsrollen so spezifiziert sind, dass die kooperierenden Akteure entweder alle ihr Ziel erreichen oder alle ihr Ziel verfehlen. Die zweite Bedingung stellt eine Erfolgskopplung der kooperierenden Aktivitäten dar und stellt ein wesentliches Kooperationsprinzip dar.

Das *Kooperationsprinzip* lautet: Eine Kooperationsrolle muss so spezifiziert sein, dass ein Akteur in ihr genau dann sein Ziel erreicht, wenn jeder zugehörige Kooperationspartner ebenfalls sein Ziel erreicht (*Erfolgskopplung*). Ein Kooperationspartner, der sein Aktivitätsziel erreichen will, muss sich dann genau so verhalten, dass auch jeder zugehörige Kooperationspartner sein Ziel erreicht. Aufgrund des Kooperationsprinzips kann man von „demselben Ziel aller kooperierenden Partner“ sprechen. Man definiert dann das „Kooperationsziel“ als die aggregierte Menge der Ziele aller an einer Kooperation beteiligten Akteure.

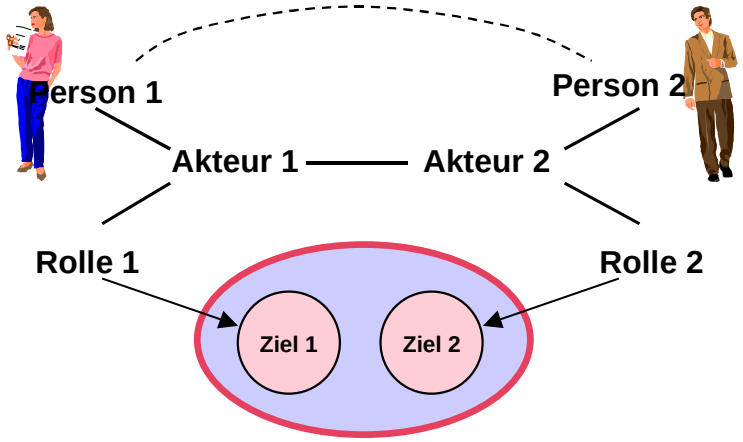

Abb. 10: Kooperation mit gemeinsamem Ziel

Beispiel für ein Kooperationsziel ist ein *Vertrag*, der von allen vertragschließenden Parteien wortgleich angenommen wird. Die Kooperationsrollen sind konfliktfrei in bezug auf das gemeinsame Kooperationsziel. Eine Person, die in eine Kooperation eintritt, ist zum Einhalten des Kooperationsprinzips verpflichtet. Die Verletzung des Kooperationsprinzips ist ein Sicherheitseinbruch. Ein verlässliches Telekooperationssystem schützt seine Teilnehmer vor Sicherheitsangriffen gegen das Kooperationsprinzip. Für E-Commerce kann der Schutz in der richtigen Verteilung von Beweisen aufgrund der jeweiligen Verpflichtungssituation bestehen („Gleichgewichtsprinzip“).

Die Semantik des Kooperationsziels kann allerdings durchaus verschieden sein, d.h. die Kooperationspartner verfolgen im allgemeinen unterschiedliche und sogar gegensätzliche Zwecke mit demselben Kooperationsziel. Ein Vertragsinhalt, zum Beispiel, reflektiert im allgemeinen die unterschiedlichen Interessen der Vertragspartner.

In Grimm und Ochsenschläger (2000) wird eine einfache Auftragskooperation mit Hilfe formaler Sprachen und endlicher Automaten modelliert: Ein Käufer und ein Verkäufer tauschen nach bestimmten Regeln eines Geschäftsvertrags Ware (result) und Geld (money) aus. Sie verwenden dabei ein Kommunikationssystem, das dafür sorgt, dass das Senden einer Nachricht von der einen Seite den Empfang der Nachricht auf der anderen Seite zur Folge hat.

Der Geschäftsvertrag schreibt den verbindlichen Austausch von Ware und Geld in einer Reihe fest vorgegebener Kommunikationsschritte vor. In diesem Beispiel gilt die Variante „erst die Ware, dann das Geld“. Die zugehörigen Nachrichten sind die Abgabe (send) und Annahme (receive) von Angebot (offer), Auftrag (order), Ware (result) und Geld (money).

Der Käufer verfolgt das Ziel, die Ware zu erhalten (*r_result*), der Verkäufer verfolgt das Ziel, das Geld zu erhalten (*r_money*). Um einen Kooperationsverlauf zu unterstützen, in dem entweder jeder Partner oder keiner sein Ziel erreicht, akzeptiert jeder der beiden Partner eine Verpflichtung, die den Partner im richtigen Moment ins Ziel führt. Der Verkäufer ist verpflichtet, die Aktionsfolge *s_offer r_order* auf seiner Seite mit dem Senden der Ware *s_result* fortzusetzen. Der

Käufer ist verpflichtet, die Aktionsfolge *s_order r_result* auf seiner Seite mit dem Senden des Geldes *s_money* fortzusetzen.

In dem Zusammenspiel zwischen Verpflichtungen und Zielen ergibt sich der ideale Kooperationsdurchgang durch das globale Wort *s_offer r_offer s_order r_order s_result r_result s_money r_money*, in dem beide Partner ihr Ziel erreichen. Hingegen sind auch andere Kooperationsdurchgänge erlaubt, in denen der Käufer Angebote ablehnt oder ignoriert. Diese sind im Sinne der Geschäftsbedingungen geregelte Abbrüche.

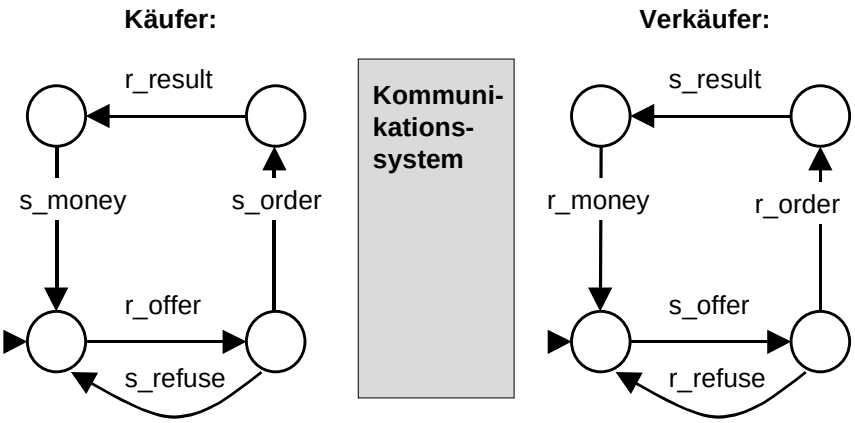

Abb. 11: Eine einfache, faire Verkaufskooperation

Ein anderes Beispiel für den Unterschied zwischen dem gemeinsamen Kooperationsziel und den individuell mit dem Kooperationsziel verfolgten Zwecken stellt das gemeinsame Spiel, etwa das Brettspiel oder Kartenspiel, dar. Das Spiel ist Vorbild des Wittgensteinschen Sprachspiels und des hier vorgestellten Kooperationsmodells. Das Kooperationsziel im Spiel ist das regelgerechte und gemeinsame Erreichen eines Spielendes. Auch im Angesicht einer Niederlage muss ein Verlierer sich an dieses Ziel halten, wenn nicht das gesamte Spiel zerstört werden soll. Der individuelle und konfliktträchtige inhaltliche Sinn und Zweck, den ein jede Spieler verfolgt, besteht darin, das Spiel gegen die Mitspieler zu gewinnen. Die Spielregeln und das regelgerechte Spielende sind allen Spielern gemeinsam. Aber die Zwecke sind gegensätzlich: die einen gewinnen, die anderen verlieren. Die Spielregeln sind in einer Spielanleitung spezifiziert, Gewinnstrategien gewöhnlich nicht. Gewinnstrategien beruhen auf persönlicher Erfahrung.

9. Risiko als Gegenstand von E-Commerce

E-Commerce darf Risiken nicht ausschalten, sondern muss sie handhabbar machen, denn Risiko ist der Gegenstand von geschäftlichem Handeln. Allerdings ist damit das inhaltliche Risiko des Gewinns gemeint, nicht das Risiko des Vertragsbruchs. Gegen formalen Vertragsbruch muss ein Handelssystem, und also auch E-Commerce, Sicherheit bieten. Das ist mit „handhabbar“ gemeint: man muss sich mit Hilfe von E-Commerce auf das Geschäftsrisiko einlassen können.

E-Commerce ist wie jede wertvolle Kooperation interessenabhängig. Die Geschäftspartner haben das Interesse, ihr Vermögen zu erhalten oder zu erhöhen. Dabei sehen die Partner in erster Linie auf ihre eigenen Werte und nehmen Wertverlust der Partner in Kauf. Es ist die Absicht eines Aktienhändlers, den Wert seines Depots auf Kosten aller anderen Börsenteilnehmer zu erhöhen. Im E-Commerce kommunizieren also Partner mit unterschiedlichen, ja gegensätzlichen Interessen. Zwar sind die Kommunikationsinhalte, also die Börsenkurse, um in diesem Beispiel zu bleiben, für alle Personen dieselben. Die Werte aber, die sich mit dem Besitz von Aktien verbinden, unterliegen der semantischen Interpretation und der Gewinnabsicht der Börsenteilnehmer. Sowohl Interpretationen als auch Absichten können aber vollkommen verschieden, ja geradezu einander entgegengesetzt sein.

Allgemein ausgedrückt: Die syntaktischen *Daten*, die im E-Commerce (und jeder anderen wertvollen Kommunikation) ausgetauscht werden, sind für alle dieselben. Die semantischen Inhalte der Daten, die diese zu wertvollen *Informationen* machen, unterscheiden sich aber je nach Interpretation und Absicht der Kommunikationspartner. Während die Syntax bei allen Kommunikationspartnern dieselbe ist, kann sich die Semantik unterscheiden.

Sicherheit bezieht sich auf Werte. Wert ist ein semantisches Konzept. Während der Geschäftsabschluss (Syntax) für alle derselbe ist, ist der damit verbundene Wert (Semantik) verschieden. Was der eine in einem Geschäft gewinnt, kann der andere verlieren, und das kann gerade der Inhalt eines Geschäftes sein. Sicherheit beruht auf Interessenkonflikten. Interessenkonflikte und ihr Ausgleich sind aber der Gegenstand von Geschäftskommunikation.

Im globalen E-Commerce muss man damit rechnen, dass die andere Seite sich nicht wohl verhält. Durch ein global anerkanntes *Rechtssystem* und mit den richtigen *Beweisen* zum richtigen Zeitpunkt einer Transaktion kann man sich dennoch darauf einlassen, wenn die *lokale Implementierung* der Kommunikationstechnik sauber ist. Dann kann nämlich jeder Teilnehmer wie im traditionellen Handel erkennen, auf wen er sich verlassen kann, und entscheiden, mit wem er Handel treiben will. Fehlverhalten ist beweisbar. Wie gewohnt kann dann das Rechtssystem als Auffangbecken zum Ausgleich von Fehlverhalten dienen.

Literatur

BSI (1998): Bundesamt für Sicherheit in der Informationstechnik: Virtuelles Geld – eine globale Falle? SecuMedia Verlag Ingelheim, BSI Bonn, 1998, 314 S.

D. Comer: Internetworking with TCP/IP, Prentice-Hall, Englewood Cliffs, NJ, 1988.

DUD (1999): Schwerpunkt Zahlungssysteme. In: Datenschutz und Datensicherheit (DuD) 1/99, Vieweg, Wiesbaden, Januar 1999. Besonders: Hagemann u.a.: Sicherheit und Perspektiven der elektronischen Zahlungssysteme.

K. Gödel: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. Monatshefte für Mathematik und Physik, 38 (1931), 173-198.

R. Grimm (1994): Sicherheit für offene Kommunikation – Verbindliche Telekooperation. B.I. Wissenschaftsverlag, Mannheim 1994.

R. Grimm, P. Ochsenschläger (2000): Elektronische Verträge und ihre verbindliche Aushandlung – ein formales Modell für verbindliche Telekooperation. In G. Kappel, G. Müller, F. Schober (Hrsg.): Informatik Forschung und Entwicklung (IFE), Themenheft „Electronic Commerce“, Oktober 2000, 182-192.

D.R. Hofstadter (1999): Gödel, Escher, Bach, ein endloses geflochtenes Band. Klett-Cotta, 15. Aufl. 1999, 844 S.

V. Kessler; S. Mund (1993): Sicherheitsmodelle – Baupläne für die Entwicklung sicherer Systeme. Arbeitspapier der Siemens AG, ZFE ST SN 3, München Nov 1993, 104 Seiten.

K. Schmeh (1998): Safer Net: Kryptographie im Internet und Intranet. dpunkt Verlag, Heidelberg 1998, 434 Seiten.

B. Schneier (1996): Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd Ed. Wiley & Sons, Chichester 1996, 758 p.

J. R. Searle, F. Kiefer, M. Bierwisch (1980): Speech act theory and pragmatics. Synthese language library. Dordrecht (u.a.), Reidel (Niederlande), 1980, 317 Seiten.

J. R. Searle, D. Vanderveken (1989): Foundations of illocutionary logic. Cambridge University Press, Cambridge, 1989, 227 Seiten.

T. Socolofsky, C. Kale (1991): A TCP/IP Tutorial, RFC1180, January 1991, available from any RFC storage, e.g., ftp://ftp.isi.edu/in-notes/rfc1180.txt

SSL (1996), A. Freier, P. Karlton, P. Kocher: The SSL Protocol, (Secure Socket Layer), Version 3.0. Internet Draft, 18 Nov 1996, 63 pages, draft-freier-ssl-version3-02.txt. Deleted from Internet-drafts server. Available from http://home.netscape.com/eng/ssl3/. Included in Transport Layer Security (TLS) standardization of the IETF, http://www.ietf.org/html.charters/tls-charter.html

WAP Forum (2000): WAP – Wireless Application Protocol: http://www.wapforum.org, 2000.

L. Wittgenstein (1922): Tractatus logico-philosophicus. Dt.-engl. Ausgabe London 1922 (Frankfurt 1960). Abgedruckt z.B. in Edition Suhrkamp Nr. 12, 1. Auflage, Frankfurt 1964, 115 Seiten.

L. Wittgenstein (1953): Philosophische Untersuchungen (Philosophical Investigations). Hrsg.: G.E.M. Anscombe, R.Rhees, dt.-engl. Ausgabe Oxford 1953 (Frankfurt 1960). Abgedruckt z.B. in Suhrkamp Taschenbuch Nr. 14, 1. Auflage, Frankfurt 1971, 268 Seiten.

01 Rüdiger Grimm, “Vertrauen im Internet – Wie sicher soll E-Commerce sein?“, April 2001, 22 S.
TU Ilmenau, Institut für Medien- und Kommunikationswissenschaft, ruediger.grimm@tu-ilmenau.de

TU Ilmenau – Institut für Medien- und
Kommunikationswissenschaft
Am Eichicht 1, 98693 Ilmenau