

## **Folgen mangelhafter Sicherheitsvorkehrungen bei elektronischen Zahlungsverkehrssystemen – Ergebnisse eines diskursiven TA-Projekts**

von Peter Zoche, Dirk-Michael Harmsen und Sven Kornetzky, Fraunhofer-Institut für Systemtechnik und Innovationsforschung (ISI), Karlsruhe

Das Fraunhofer-Institut für Systemtechnik und Innovationsforschung (ISI), Karlsruhe, hat in den vergangenen zwölf Monaten für das Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, ein Projekt durchgeführt, das sich mit den "Folgen fehlender oder unzureichender Sicherheitsvorkehrungen im elektronischen Zahlungsverkehr" auseinandersetzt. Die Ergebnisse sind in einem umfangreichen Bericht, der in diesen Tagen der Öffentlichkeit zugänglich wird, dokumentiert.<sup>1</sup> Der vorliegende Beitrag umreißt den Forschungsgegenstand, stellt die methodische Vorgehensweise vor, faßt wesentliche Ergebnisse zusammen und stellt Handlungsoptionen und Leitlinien vor, die zu einer umfassenderen Informationstechnik-(IT-)Sicherheit im Umgang mit neuen elektronischen Zahlungssystemen führen können.

### **1. Untersuchungsgegenstand und Projektziele**

Nicht allein der Einsatz und die Diffusion, sondern vor allem auch die Zugangsmöglichkeiten zu und der Umgang mit neuen Informations- und Kommunikationstechnologien sind wesentliche Kriterien für die Bestimmung künftiger gesellschaftlicher Beziehungen und Kulturen. In diesem Kontext und unter Berücksichtigung der sich zunehmend schwieriger gestaltenden Beherrschbarkeit und Kontrolle der Systeme erhält der Umgang mit Risiken sowie deren gesellschaftliche Akzeptanz eine vorrangige Bedeutung. Die Verletzlichkeit der Gesellschaft durch die Verwundbarkeit technischer Systeme fundiert die Bedeutung eines umfassenden Sicherheitsbegriffs, um der Komplexität des sozio-technischen Systems gerecht zu wer-

den. Die Anforderungen an die Sicherheit der Systeme wachsen mit ihrer Verbreitung und der Abhängigkeit von ihnen.

Im Finanzsektor ist die Informatisierung traditionell weit fortgeschritten. Diese Entwicklung hat gleichzeitig die Ausfallrisiken und Mißbrauchsmöglichkeiten erhöht. Die Abhängigkeit der Gesellschaft von einer funktionierenden Kreditwirtschaft verlangt aber eine hohe Sicherheit der Systeme, mit denen sie operiert, worauf sich die essentielle volkswirtschaftliche Relevanz technischer und organisatorischer Sicherheitsvorkehrungen begründet. Die Bemühungen nach einer weiteren Automatisierung der Geldgeschäfte und die Suche nach neuen Vertriebsformen sind – insbesondere im Privatkundenbereich – stark auf das Internet gerichtet und werden daher wesentlich von dessen Erfolg bestimmt sein.

Gleiches gilt für die unter dem Schlagwort *electronic commerce* zusammengefaßten Aktivitäten des elektronischen Geschäftsverkehrs mit seinen Herausforderungen und Chancen für Unternehmen und Verbraucher sowie die Volkswirtschaft in ihrer Gesamtheit. Bestimmend für den erwünschten Erfolg des Internet ist das Vertrauen aller Akteure in dessen Sicherheitsinfrastruktur. Dieses muß aber – das bestätigen empirische Untersuchungen<sup>2</sup> – gegenwärtig noch als unzureichend angesehen werden. Demnach kommt es darauf an, nach gesellschaftspolitischen Effekten neuer Technologien zu fragen und gesellschaftliche Schutzanforderungen zu bestimmen, um so IT-Sicherheit marktfähig, also vertrauensstiftend und akzeptanzfördernd zu gestalten.

<b>Projektziele</b>
<ul style="list-style-type: none"> <li>• Bestandsaufnahme elektronischer Zahlungsverkehrssysteme und deren Probleme</li> <li>• Analyse der Verletzbarkeit von IT-Systemen im elektronischen Zahlungsverkehr</li> <li>• Aufzeigen von Folgen unzureichender IT-Sicherheit</li> <li>• Beschreibung von Gestaltungs- und Handlungsoptionen</li> </ul>

Aufgabe des Projekts war es, im Rahmen eines diskursorientierten Forschungsansatzes zur Technikfolgen-Abschätzung die Spannbreite möglicher Folgen fehlender oder unzureichender IT-Sicherheitsvorkehrungen im elektronischen Zahlungsverkehr aufzuzeigen und in einer Eingrenzung auf wesentliche Fragestellungen kritisch zu beleuchten; diese Analyse ist daran ausgerichtet, mögliche Problemlösungen bzw. weiteren, vertiefenden Untersuchungsbedarf aufzuzeigen.

## 2. Methodischer Ansatz

Die Arbeitsmethodik des Projekts war am Konzept der Technikfolgen-Abschätzung (TA) unter Berücksichtigung der erweiterten IT-Sicherheitsbetrachtung ausgerichtet. Im Sinne einer *handlungsorientierten TA* wurden nicht nur mögliche Entwicklungslinien identifiziert, sondern auch handlungsorientierte Maßnahmenbündel herausgearbeitet. Dieser Ansatz wurde durch das Element des *strukturierten Diskurses* erweitert, womit ein zeitstabiler, verlässlicher Dialog breiter Akteurskreise über deren Ziele, Prioritäten und Instrumente ermöglicht wurde. Der Studie wurde ein ganzheitliches Sicherheitsverständnis zugrundegelegt, wodurch die *Sicherheitsbetrachtung in einem erweiterten sozio-technischem Kontext* vollzogen werden konnte.

Verlässlichkeit und Verletzlichkeit sind in diesem Zusammenhang die beiden zentralen Begriffe. Während unter Verlässlichkeit die technische Ausrichtung von IT-Sicherheit subsumiert wird, fokussiert Verletzlichkeit auf die wirtschaftlichen, rechtlichen und gesellschaftlichen Auswirkungen und Schadenspotentiale, die nicht nur durch Mißbrauch, sondern auch und insbesondere durch eine alltägliche, normkonforme Anwendung entstehen können.

## 3. Projektverlauf

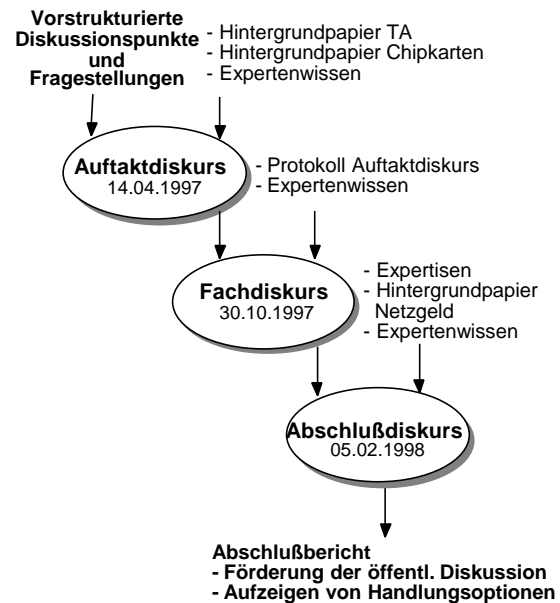
Auf Grundlage einer vom ISI-Projektteam erarbeiteten Grobstrukturierung des Untersuchungsgegenstandes wurde in einem *Auftaktdiskurs* mit einem interdisziplinär zusammengesetzten Personenkreis von Fachexperten<sup>3</sup> über die inhaltliche Fokussierung und die praktische Umsetzung des Forschungsvorhabens beraten. Im Verlauf dieses Diskurses wurden vielfältige

Problembereiche konkretisiert, neue Fragestellungen identifiziert und Handlungsnotwendigkeiten benannt (z.B. Annahmepflicht von Zahlungsmitteln, Wahlfreiheit über die Verwendbarkeit von Zahlungsmitteln durch den Verbraucher, Stärkung der Verantwortlichkeit des Staates für eine sichere Zahlungsverkehrsinfrastruktur zum Nutzen des Verbrauchers, Offenlegung der Sicherheitsmerkmale für öffentliche Systeme, Qualifizierung der Nutzer). Für den Fortgang des Projekts wurde die Notwendigkeit herausgestellt,

- prioritär den Planungs- und Realisierungsstand neuer elektronischer Zahlungsverkehrssysteme möglichst vollständig zu erfassen,
- allgemeine und übergreifende Sicherheitsanforderungen für elektronische Zahlungsverkehrssysteme zu bestimmen sowie
- geld- und währungspolitische Fragen und damit im Zusammenhang stehende mögliche systemische Risiken neuer Zahlungsverkehrssysteme zu analysieren.

Der Diskussionsverlauf des Auftaktdiskurses und die eingebrachten Arbeitspapiere wurden vom Projektteam analysiert und zusammenfassend dokumentiert. Zur Unterstützung des Projektteams wurden Kooperationspartner gewonnen, die im Rahmen von Expertisen vertiefende Analysen ausarbeiteten. Ergebnisse dieser Analysen wurden in einem *Fachdiskurs* vorgestellt, an dem verschiedene Meinungs- und Interessengruppen teilnahmen (u.a. Hersteller- und Betreiberunternehmen, Verbraucherverbände, Ministerien). Diese Veranstaltung diente der *Überarbeitung bzw. der Vertiefung* der erarbeiteten Positionen. Im weiteren Projektverlauf wurden vorläufige Schlußfolgerungen und Handlungsoptionen erarbeitet, die als Orientierungswissen für den weiteren Einführungsprozeß elektronischer Zahlungsverkehrssysteme dienen sollen. Diese Ausführungen wurden in einem öffentlichen *Abschlußdiskurs* präsentiert, zu dem international eingeladen wurde. Die Präsentationen und Diskussionen dieses Tages sind in den Abschlußbericht eingeflossen.

Eine Übersicht über den gesamten Projektverlauf gibt die nachfolgende Abbildung.



**Abbildung:** Schematische Übersicht zum Projektverlauf

#### 4. Inhaltliche Schwerpunkte

Charakteristisch für die gegenwärtige Phase der Automatisierung des Zahlungsverkehrs sind die Entwicklung, Erprobung und schrittweise Einführung *multifunktionaler Kartensysteme* sowie die *softwarebasierten Zahlungsverkehrssysteme*. Bis Ende der 80er Jahre hat sich die Automatisierung vorwiegend auf Zahlungsvorgänge innerhalb des Kreditgewerbes sowie zwischen dem Kreditgewerbe und seinen Kunden (Privat- und Geschäftskunden) konzentriert. Mit der Einführung kartengestützter elektronischer Zahlungen im Handel und Dienstleistungsgewerbe (POS) wird die Automatisierung auf Zahlungsvorgänge erweitert, die außerhalb der Kreditwirtschaft und heute überwiegend noch mit Bargeld abgewickelt werden. Folgende *Kartenarten* kommen dabei zum Einsatz: vorausbezahlte Wertkarten, Debit-Karten, und Kreditkarten. Sie positionieren sich in Abhängigkeit des Transaktionsvolumens sowie der Bonität des Karteninhabers unterschiedlich im Markt. Die bundesweit größte Verbreitung weist mit ca. 50 Millionen die *ec-Karte* (Debit-Karte) auf.

Mit der technischen Weiterentwicklung der Magnetstreifenkarte zur mit Speicherchip und Mikroprozessor ausgestatteten Chipkarte erschließen sich neue Anwendungsfelder für Kartensysteme. Die Chipkarte kann auf folgende

Vorteile verweisen: höhere Sicherheit gegen Angriffe auf das Zahlungsverkehrssystem, niedrigere Kommunikationskosten durch Off-line-Autorisierung, zusätzliche und durch Verschlüsselung sichere Datenspeicherung auf der Chipkarte, verkürzte Abwicklungszeit an der POS-Kasse und vielfache Verwendbarkeit als Geldkarte, Zugangskarte, Ausweis etc. (*Multi-funktionskarte*).

Weltweit gibt es eine Vielzahl von Projekten, in denen Chipkarten als Geldkarten (elektronische Geldbörsen) eingesetzt werden. Die Studie gibt einen Überblick über zahlreiche solcher Projekte. Für den deutschen Verbraucher sind derzeit drei Systeme von Interesse [vgl. hierzu auch den Beitrag von Gentz]:

- Die von den deutschen Kreditinstituten herausgegebene *GeldKarte* als Kombination von ec-Karte oder Bankenkundenkarte mit einem Chip,
- die von der Deutschen Telekom AG, der Deutschen Bahn AG und dem Verband Deutscher Verkehrsunternehmen emittierte *PayCard* sowie
- die von einem Verbund der Unternehmen Electronic Banking Systems, Orga Kartensysteme und der Krone Kommunikationsgesellschaft angebotene *P-Card*.

Unter softwarebasierten Zahlungsverfahren waren zunächst vor allem Verfahren zu verstehen, die es Kunden ermöglichen, Zahlungsverkehrsvorgänge in elektronischer Form ihrem Kreditinstitut zu übermitteln (*electronic banking*). Seit dem Beginn der kommerziellen Nutzung des Internet als virtueller Umschlagplatz für Waren und Dienstleistungen wird die Entwicklung von Verfahren forciert, die die Abwicklung finanzieller Transaktionen auf diesem Marktplatz erlauben. Die besondere Herausforderung liegt in der Natur des Internet als offenes Netzwerk, das im Vergleich zu geschlossenen Netzwerken besondere Sicherheitsprobleme aufwirft. Die folgenden Ansätze lassen sich im Bereich der softwarebasierten Verfahren unterscheiden:

- kreditkartenorientierte Verfahren,
- Scheck- und lastschriftorientierte Verfahren,
- bargeldähnliche Verfahren,
- Micropayment-Systeme.

Hinzu kommen aktuelle Entwicklungen im Bereich des *electronic banking* (Homebanking) sowie systemübergreifende Vorschläge zur Abwicklung von Finanztransaktionen. In Deutschland erscheinen aufgrund von Pilotprojekten marktmächtiger Kreditinstitute die folgenden Systeme als für die Zukunft besonders aussichtsreich:

- *SET (Secure Electronic Transaction)* ist ein internationaler de facto-Standard für Kreditkartenzahlungen im Internet, der in Deutschland bspw. von der Commerzbank und der Gesellschaft für Zahlungssysteme unterstützt wird.
- *ecash* ist ein bargeldähnliches Verfahren der Firma DigiCash, das von der Deutschen Bank getestet wird.
- *CyberCash* bietet eine umfangreiche Lösung des gleichnamigen Unternehmens für verschiedene Zahlungsverfahren unter einer einheitlichen Oberfläche. In der Bundesrepublik wird dieses System z. B. von der Dresdner Bank getestet und umfaßt – bzw. soll zukünftig umfassen – ein kreditkartenorientiertes Verfahren, das auf SET und CyberCash basiert, ein bargeldähnliches Verfahren namens CyberCoin sowie das Lastschriftverfahren edd (electronic direct debit).

In Zukunft wird die Unterteilung in Hard- und Softwaresysteme obsolet werden, da kartengestützte Lösungen für Internettransaktionen am heimischen PC entwickelt werden, wie etwa der Einbezug von Chipkarten in SET-Anwendungen.

Im Vordergrund der Analysen einer erweiterten Sicherheitsbetrachtung stehen die Aspekte Komplexität und Beherrschbarkeit, Verwendbarkeit und Funktionalität, Kontroll-Potential sowie Risiken aus Anwenderperspektive, wobei zwischen den technischen Systemen und den Anwendungen differenziert wird.

Elementar orientiert sich die Beurteilung neuartiger elektronischer Zahlungsverfahren an Kriterien, die bereits für die Beurteilung herkömmlicher Zahlungsinstrumente relevant sind: Annahmezwang, niedrige bis keine Kosten, einfache und unkomplizierte Übertragung von Geldeinheiten, direkte Übersicht über die Geldmenge in der eigenen Börse, einfache Geldbeschaffungsformen, Anonymität, Möglichkeit

zum Laden selbstgewählter und insbesondere niedriger Beträge.

Insgesamt existiert eine Vielzahl von Akteuren, z.B. Verbraucher (Kunden, Konsumenten), Händler, Verkäufer, Kreditinstitute, Kreditkartengesellschaften, Systementwickler, -betreiber, Zentralbank und Staat, deren interessengebundene Anforderungen an die Gestaltung der Systeme berücksichtigt werden müssen.

Um die *Verlässlichkeit* im elektronischen Zahlungsverkehr einschätzen zu können, wurden die technische und die technisch-organisatorische Betrachtungsebene der IT-Sicherheit analysiert. Entsprechende Kriterien für eine Beurteilung der IT-Sicherheit können in Anlehnung an den Kriterienkatalog von ITSEC (Information Technology Security Evaluation Criteria) formuliert werden, und es lassen sich daraufhin Bedrohungsklassen für IT-Systeme bilden:

#### *I Essentielle Bedrohungen*

Bedrohungen, die die Funktion des Zahlungssystems in seinem Kern betreffen und gegen die daher unbedingt Gegenmaßnahmen zu ergreifen sind.

#### *II Relevante Bedrohungen*

Bedrohungen, die eine ernsthafte Gefährdung des Systems oder dessen Benutzer darstellen, weshalb Gegenmaßnahmen als wichtig zu erachten sind.

#### *III Tolerierbare Bedrohungen*

Bedrohungen, denen auch herkömmliche Zahlungssysteme nicht ausreichend begegnen können und die daher gegebenenfalls tolerierbar sind.

Die Bedrohungen lassen sich abwehren, wenn systemimmanente Schwächen abgebaut werden. Für den Bereich der elektronischen Zahlungsverkehrssysteme werden dazu folgende Maßnahmen vorgeschlagen: Verwendung kryptografischer Zertifikate zur Identifikation des Zahlenden, Einsatz erkennbar zertifizierter Endgeräte, Verwendung von Qualitätsstandards während der Entwicklung, genormte Schnittstellen für die Integration von Kryptofunktionen, keine Speicherung personenbezogener Daten, Verwendung von Pseudonymen zur Kontoführung, Backup-Konzepte bei Verlust, Abgrenzung der einzelnen Funktionen multifunk-

tionaler Chipkarten, Anwenderschulungen zur Erlernung des sachgemäßen Umgangs mit den Zahlungsmitteln sowie der zu nutzenden Infrastruktur (Endgeräte, wie Personal Computer, Lade- und Lesegeräte etc.).

Um das *Verletzlichkeit*spotential von Systemen zu ermitteln, sind die rechtliche, ökonomische und gesellschaftliche Ebene zu betrachten. Überlegungen hierzu sind in den abschließenden Teil dieses Beitrags eingegangen.

## **5. Chancen und Herausforderungen elektronischer Zahlungsverfahren**

Es ist zu betonen, daß die Verlagerung von Geschäftsprozessen in ein globales Netzwerk wie das Internet und mithin auch der neuartige elektronische Zahlungsverkehr neben Risiken resp. Herausforderungen auch zahlreiche Chancen für sämtliche Akteure mit sich bringt. Bei wirksamer Erhöhung der Verlässlichkeit der technischen Systeme sowie einer Eingrenzung der Verletzlichkeit im gesellschaftlichen Kontext lassen sich neben zahlreichen individuellen die folgenden volkswirtschaftlich relevanten Chancen elektronischen Geldes benennen:

- Schaffung neuer Nachfragesektoren als Folge des Aufbaus sowie der Wartung entsprechender Infrastrukturen,
- Reduzierung regionaler Standortnachteile infolge einer Globalisierung der Endverbrauchermärkte mittels "Netzgeld",
- Schaffung von Arbeitsplätzen in technologielevanten Bereichen,
- Effizienzgewinne durch eine verbesserte Transaktionsabwicklung.

Der *Datenschutz* steht vor dem Hintergrund der technischen, rechtlichen und ökonomischen Entwicklung sowie unter gesellschaftlichen und psychologischen Aspekten vor der Herausforderung, das Recht des einzelnen auf informationelle Selbstbestimmung immer wieder einzufordern und zu schützen. Entsprechende rechtliche Regelungen sind an die neuen Gegebenheiten anzupassen bzw. bestehende Regelungen umzusetzen. Eine besondere Herausforderung stellt im Kontext elektronischer Zahlungsverkehrssysteme die Bereitstellung anonymer und pseudonymer Zahlungsverfahren dar.

Dem Verbraucher können aus einem Markt, auf dem sämtliche Teiltransaktionen von der Information über Produkte bis hin zum Bezahlen elektronisch ausgeführt werden, Vorteile erwachsen, sofern die Risiken und Hemmnisse, die zunächst einmal dessen Stellung schwächen, minimiert bzw. beseitigt werden. Es sind dafür technische Anforderungen, rechtliche Regelungen, organisatorische Forderungen und soziale Aspekte zu beachten und Lösungen für diesbezüglich offene Fragen zu finden.

Elektronisches Geld birgt gewisse *volkswirtschaftliche Risiken*, die sich allerdings nur zum Teil von denen herkömmlichen Geldes unterscheiden. Technische Sicherheitsstandards sind geeignet, diese Risiken zu vermindern, wogegen dies für nationale Regulierungen nur bedingt gilt. Grund hierfür ist der transnationale Charakter des Internet und des Geldwesens. Internationale Absprachen scheinen daher adäquater als nationalstaatliche Regelungen. Es kann prognostiziert werden, daß elektronisches Geld zu mehr Wettbewerb im Geldmarkt, mehr Eigenverantwortung des einzelnen, mehr Markt und weniger Regulierungen führen wird.

Electronic und Direct Banking sowie elektronisches Geld werfen unter dem Aspekt der *Geldwäsche* gewisse Risiken auf, da sie bisherige Grundsätze in der Geldwäsbekämpfung (direkter Kontakt Bank – Kunde, Bargeldansatz) zukünftig obsolet erscheinen lassen. In der Prävention krimineller Angriffe im Sinne der Geldwäsche liegt die Gefahr, daß individuelle Persönlichkeitsrechte sowie der Grundsatz der Verhältnismäßigkeit nicht gewahrt werden. Es gibt in diesem Bereich gegenwärtig keine Lösung, die den Interessen aller Akteure entspricht. Maßnahmen, die etwa von der Financial Action Task Force (FATF) vorgeschlagen werden (Höchstbeträge für Transaktionen, keine transnationalen Zahlungen, keine peer-to-peer-Transaktionen) senken die Attraktivität elektronischen Geldes und damit möglicherweise seine Akzeptanz. Außerdem können sie den globalen Handel erschweren.

Getrieben von der technischen Entwicklung im Zahlungsverkehr dehnt sich die *Rationalisierung im Kreditgewerbe* zunehmend auf das Privatkundengeschäft aus. Die Folgen sind vielseitig: radikaler Umbau der Branchenstruktur sowie massive Arbeitsplatzverluste sind die beiden erheblichsten. Für die Beschäftigten ist

dies mit der Auflösung vertrauter Strukturen und dem Verlust an Sicherheiten verbunden.

Die *Besteuerung* steht angesichts der Virtualisierung von Geschäftsprozessen vor einem Dilemma. Einerseits soll sie staatliches Einkommen sichern, volkswirtschaftliche Steuerungsfunktionen (bedingt) ausüben und nach dem Grundsatz der Wettbewerbsneutralität erfolgen. Andererseits ergeben sich Probleme bei der Zuordnung von Personen und Unternehmen zu realen Standorten oder bei der Identifikation, wenn zunehmend anonyme und pseudonyme Formen der Kommunikation und Transaktionsabwicklung Verwendung finden. Auswege, um eine "Erosion der Steuerbemessungsgrundlage" zu verhindern, existieren bisher keine, lediglich Ansätze, die sich allerdings (berechtigter) Kritik ausgesetzt sehen, da sie mit zu hohem finanziellem und administrativem Aufwand zu betreiben wären und außerdem Persönlichkeitsrechte gefährden (Datenschutz). Konsens herrscht zumindest in der Ansicht, die Entwicklung des Internet und des elektronischen Handels nicht durch neuartige Steuern zu behindern.

Eine in wachsendem Maße auf virtuelle Kommunikations- und Handelsstrukturen setzende Industriegesellschaft muß die entsprechenden systemischen Voraussetzungen schaffen und *Anwenderkompetenz* entwickeln, die eine allgemeine Inbesitznahme und Nutzung der neuen Technologien – hier Zahlungsverkehrssysteme – erlauben. Schlagwortartig seien in diesem Zusammenhang genannt: Girokonto für jedermann, öffentlich zugängliche Terminals, "digitale Briefftasche" für alle, transparente und verständliche Informationen, Vermittlung medienkompetenten Handelns.

Für eine ganze *Reihe rechtlicher Aspekte* elektronischen Geldes, wie etwa seine Rechtsnatur oder die Frage der Rechtsbeziehungen zwischen beteiligten Akteuren, besteht Diskussions- und Klärungsbedarf. In einem übergeordneten Kontext steht die generelle Frage nach geeigneten Regelungsstrategien in einem Raum (globale Netzwerke), in dem nationale Souveränität aufhört zu existieren. Es gilt als sicher, daß der Staat zunehmend in eine Strukturverantwortung hineinwächst, bei der er dem Bürger die Voraussetzungen zu dessen wirkungsvollem Selbstschutz in die Hand geben muß.

Prämisse für derartige Empfehlungen ist die Einsicht, daß die Gewährleistung von Sicherheit an den Bedürfnissen verschiedener Akteure orientiert sein sollte. Das Konzept der mehrseitigen Sicherheit beinhaltet, daß unterschiedliche Sicherheitsanforderungen der beteiligten Akteure auf einen gemeinsamen Anwendungskontext zu beziehen sind und auf dieser Grundlage – unter Erfassung übergeordneter gesellschaftlicher Maßstäbe – gegeneinander abgewogen werden sollten.

Verbraucherschutzverbänden, Interessenvertretungen von Arbeitnehmern und staatlichen Institutionen, hier insbesondere Datenschutzbehörden, kommt eine besondere Verantwortung zu, wenn es gilt, das Gleichgewicht der Kräfte zwischen den einzelnen Akteuren zu wahren bzw. erst herzustellen. Ohne diese Interessenwahrnehmung befindet sich der einzelne Bürger zunächst in einer vergleichsweise "schwachen Position". Die Anstrengungen sind vor allem auf Maßnahmen, die den Postulaten der informationellen Selbstbestimmung sowie der *Stärkung der Stellung des Verbrauchers* gerecht werden, zu richten.

Im Rahmen der Systemgestaltung sind *Integritätsaspekte* unter Beachtung des Prinzips der mehrseitigen Sicherheit zu berücksichtigen. Darüber hinaus sollte die angestrebte *Akzeptanz* bereits bei der Planung eines Systems auf der Basis der Identifikation von Schutzanforderungen zur Vermeidung negativer gesellschaftspolitischer Effekte im Mittelpunkt stehen. *Datensparsamkeit* und *Anonymität* sind als zentrale Gestaltungskriterien zu betrachten. Zur Umsetzung dieser Leitlinien stehen den Entwicklern zahlreiche *technische und technisch-organisatorische Hilfsmittel* zur Verfügung.

Es wird erwartet, daß sich – sofern sich die neuartigen elektronischen Zahlungsverfahren gegenüber herkömmlichen Zahlungsinstrumenten durchsetzen können – verschiedene Lösungen, die auf unterschiedlichen Ansätzen basieren, durchsetzen und sich verschiedene Einsatzfelder erschließen. Systemhersteller und -betreiber können diese Entwicklung in ihrem Sinne beeinflussen, wenn sie *Hemmnisse* und *Risiken*, die der breiten Nutzung der Verfahren entgegen stehen, mit ihren Arbeiten abbauen helfen.

Bei der Ausgestaltung des rechtlichen, ökonomischen und sozialen Fundaments für

den elektronischen Geschäftsverkehr, der eng mit generellen Fragen nach der Gestaltung der Informationsgesellschaft verbunden ist, tragen der Staat und seine Institutionen Verantwortung. Insbesondere betrifft dies die folgenden Bereiche:

- Schaffung des rechtlichen Rahmens für die Entwicklung und den Einsatz elektronischen Geldes sowie dessen Implikationen bspw. für die Geldökonomie, die Steuererhebung oder die Bekämpfung der Geldwäsche. Internationale Absprachen und Regelungen sind nationalstaatlichen vorzuziehen. Dem Bürger sind ferner Mittel in die Hand zu geben, die ihm einen ausreichenden Selbstschutz in der Welt der digitalen Netzwerke erlauben.
- Jedem einzelnen Bürger ist die Teilnahme am elektronischen Zahlungsverkehr zu ermöglichen. Die entsprechenden Voraussetzungen sind zu schaffen. Dies betrifft sowohl die (materiellen) Zugangsvoraussetzungen, die bspw. in Form einer "digitalen Geldbörse für alle" gewährleistet werden können, als auch die Vermittlung medienkompetenten Verhaltens, wozu Reformen bei der allgemeinen und beruflichen Bildung erforderlich sind – mit Lernenden und Lehrenden als Adressaten.

Das Projektteam wurde in den vergangenen Monaten von sehr vielen Personen mit Expertisen, Positionspapieren und anregenden Diskussionsbeiträgen unterstützt; für diese Mitwirkung danken wir allen Beteiligten sehr.

### Anmerkungen

- 1 Zoche, P.; Kornetzky, S.; Harmsen, D.-M. (1998): "Folgen fehlender oder unzureichender IT-Sicherheitsvorkehrungen im elektronischen Zahlungsverkehr", Fraunhofer-Institut für Systemtechnik und Innovationsforschung, Karlsruhe, Mai 1998.
- 2 Vgl. Breiter, A.; P. Zoche (1997): "Kommerzialisierung des Internet - was halten Nutzer von den Angeboten?", in: Kubicek, H. et al. (Hrsg.): Jahrbuch Telekommunikation und Gesellschaft 1997, Heidelberg: v. Decker; sowie Kornetzky, S.; Zoche, P. (1998): "Internet User Survey"; Fraunhofer-Institut für Systemtechnik und Innovationsforschung, Karlsruhe, Januar 1998.
- 3 Für diese Mitarbeit danken wir den am Diskurs beteiligten Mitarbeitern des Bundesamtes für Si-

cherheit in der Informationstechnik, Bonn, sowie folgenden extern gewonnenen Fachleuten: Bernd Beykirch, Informatikzentrum der Sparkassenorganisationen, Bonn; Wendelin Bieser, Bundesministerium des Innern, Bonn; Prof. Dr. Alfred Büllesbach, Konzernbeauftragter Datenschutz Daimler-Benz AG, Leinfelden-Echterdingen; Dr. Rüdiger Grimm, GMD, Darmstadt; Gerald Krummeck, IABG, Ottobrunn; Prof. Dr. Günter Müller, Universität Freiburg; Prof. Dr. Andreas Pfitzmann, Technische Universität Dresden; Dr. Uwe Schläger, Hamburgischer Datenschutzbeauftragter; Dr. Gerhard Weifl, Technologie- und Innovationsberatungsstelle (TIB) des DGB Hamburg.

### **Kontakt**

Dr. Peter Zoche  
Fraunhofer-Institut für Systemtechnik  
und Innovationsforschung  
Breslauer Str. 48, D-76139 Karlsruhe  
Tel.: + 49 (0) 721/6809-152  
E-mail: pz@isi.fhg.de

»