Sicherheit elektronischer Bezahlsysteme in Deutschland unter spezieller Berücksichtigung bankaufsichtlicher Besonderheiten

Zur Erlangung des akademischen Grades eines
Doktors der Wirtschaftswissenschaften
(Dr. rer. pol.)

von der Fakultät für Wirtschaftswissenschaften
der Universität Fridericiana zu Karlsruhe

genehmigte

Dissertation

von

Dipl.-Wi.-Ing. Karsten Stroborn

Tag der mündlichen Prüfung:	**17. Februar 2004**
Referent:	**Prof. Dr. Werner Rothengatter**
Korreferent:	**Prof. Dr. Andreas Geyer-Schulz**

2004

Karlsruhe

Inhaltsverzeichnis - Kurzform

Inhaltsverzeichnis

Abkürzungsverzeichnis

3-D	Three Domain
AGB	Allgemeine Geschäftsbedingungen
AGBG	Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen
AMA	Advanced Measurement Approaches, Fortgeschrittene Messverfahren
AZV	Auslandszahlungsverkehr
B2B	Business to Business
B2C	Business to Consumer
BAFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKred	Bundesaufsichtsamt für das Kreditwesen
Basel I	Basler Eigenkapitalvereinbarung
Basel II	Neue Basler Eigenkapitalvereinbarung
BAV	Bundesaufsichtsamt für das Versicherungswesen
BAWe	Bundesaufsichtsamt für den Wertpapierhandel
BBankG	Bundesbankgesetz
BCBS	Basle Committee on Banking Supervision (Basler Ausschuss für Bankenaufsicht)
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BIC	Bank Identifier Code
BIZ (BIS)	Bank für Internationalen Zahlungsausgleich, (Bank for International Settlement)
BSC	Banking Supervision Committee of the European System of Central Banks
BSE	Belegloses Scheckeinzugsverfahren
BSI	Bundesamt für Sicherheit in der Informationstechnik
CGFE	Committee on Gold and Foreign Exchange
CGFS	Committee on the Global Financial System
CLS	Continious Linked Settlement
CPSIPS	Core Principles for Systemically Important Payment Systems
CPSS	Committee on Payment and Settlement Systems
CVC	Card Validation Code
CVV	Card Verification Value
DTAUS	Datenträgeraustauschformat
DFÜ	Datenfernübertragung
EAF	Euro Access Frankfurt/Elektronische Abrechnung Frankfurt
EAL	Evaluation Assurance Level
EBA	Euro Banking Association
EBPP	Electronic Bill Presentment and Payment
(EC)BAC	European Commission Banking Advisory Committe
ECBS	European Committee for Banking Standards
EDIFACT	Electronic Data Interchange For Administration Commerce and Transport
EFSA	European Financial Services Authority (EU-Regulierungs- und Aufsichtsbehörde)
EFTPOS	Electronic Funds Transfer at the Point of Sale
EI	Exposure Indicator, Bereichsaktivität-Indikator
EL	Expected Loss, erwarteter Verlust
ELS	Euro Link System/Elektronischer Schalter
EMZ	Elektronischer Massenzahlungsverkehr
EMV	**E**uropay, **M**astercard, **V**isa (Entwickler des EMV-Chips, der zukünftig den Magnetstreifen auf Kredit-/Debitkarten ersetzen soll)
EPC	European Payments Council
ERP	Euro Retail Payment
ESZB	Europäisches System der Zentralbanken
ETSI	European Telecommunciations Standards Institute
EU	Europäische Union

E(W)G	Europäische (Wirtschafts-)Gemeinschaft
EZB (ECB)	Europäische Zentralbank, (European Central Bank)
FSAP	Financial Sector Assessment Program (der Weltbank und des IWF)
FSAP	Financial Services Action Plan (Aktionsplan für Finanzdienstleistungen der EU)
GAAP	Generally Accepted Accounting Principles
GdC	Groupe de Contact/Contact Group
GSE	Großbetrag-Scheckeinzugsverfahren
GZS	Gesellschaft für Zahlungssysteme
HBCI	Homebanking Computer Interface
IBAN	International Bank Account Number
ICBS	International Conference on Banking Supervisors
IDW	Institut Deutscher Wirtschaftsprüfer
IMA	Internal Measurement Approaches, Interne Messverfahren
IPSP	Internet Payment Service Provider
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Informationstechnologie
IWF (IMF)	Internationaler Währungsfonds (International Monetary Fonds)
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG	Kreditwesengesetz
LDA	Loss Distribution Approaches, Verlustverteilungs-Ansätze
LDCE	Loss Data Collection Exercise for Operational Risk
LGD	Loss Given Default, Ausfallquote
LGE	Loss Given that Event occurs, Verlusthöhe im Schadensfall
MaH	Mindestanforderungen an das Betreiben von Handelsgeschäften
MaK	Mindestanforderungen an das Kreditgeschäft
MT	Message Type
NZB	Nationale Zentralbank
OpVaR	Operational Value at Risk
P2P	Person to Person
PD	Probability of Default, Ausfallwahrscheinlichkeit
PE	Probability that event occurs, Schadenswahrscheinlichkeit
(PE)ACH	(Pan-europäisches) Automatisiertes Clearinghaus ((Pan-European) Automated Clearinghouse)
PIN	Personal Identification Number
POS	Point of Sale
QIS	Quantitative Impact Study
RPI	Risk Profile Index
RTGS^{plus}	Bruttozahlungssystem (Real Time Gross Settlement) der Bundesbank und gleichzeitig deutsche TARGET-Komponente
SEPA	Single European Payment Area
SET	Secure Electronic Transaction
SIPN	Secure IP Network (SWIFT)
Sound Practices	Sound Practices for the Management and Supervision of Operational Risk
SRP	Supervisory Review Process
SSL	Secure Socket Layer
STP	Straight Through Processing
S.T.E.P.S.	Straight Through Euro Payment System
S.W.I.F.T. (SWIFT)	Society for Worldwide Interbank Financial Telecommunication
TARGET	Transeuropean Automated Real-time Gross Settlement Express Transfer
TIS	TARGET Informations System
UCAF/SPA	Universal Cardholder Authentification Field/Secure Payment Application
UL	Unexpected Loss, unerwarteter Verlust
VDZ	Verband Deutscher Zeitschriftenverleger
ZKA	Zentraler Kreditausschuss

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Zahlungsverkehrslandschaft in Deutschland: Problemstellung

Die Elektronisierung des Zahlungsverkehrs ist in Deutschland durch das Zusammenspiel technologischer und marktseitiger Entwicklungen in den letzten Jahren weit vorangeschritten. Die gemeinsame europäische Währung und die damit einhergehenden institutionellen Veränderungen und rechtlichen Rahmenbedingungen haben diesen Trend deutlich verstärkt. Die Großzahlungssysteme sind in noch stärkerem Maße elektronisch basiert und supranational verknüpft als die Massenzahlungssysteme; letztere holen jedoch seit Mitte der neunziger Jahre auf.

Kosteneffiziente Abwicklung und Echt-Zeit-Verarbeitung sind die vorherrschenden Entwicklungsrichtungen im Zahlungsverkehr. Das US-amerikanische Federal Reserve System und das Europäische System der Zentralbanken (ESZB) rechnen mit weiteren Elementen der Elektronisierung des Zahlungsverkehrs durch Straight Through Processing und Electronic Bill Presentment and Payment. Sie wollen diese Entwicklung aktiv vorantreiben. Die Vision einer elektronischen Revolution, bei der digitales Geld den gleichen Stellenwert wie Bargeld hat, ist (vorerst) nicht eingetreten. Die Evolution elektronischer Zahlungssysteme hingegen ist unaufhaltsam und in der Taktfrequenz schneller geworden.[1]

Der Markt für Zahlungssystem-Dienstleistungen ist groß: Allein 2001 wurden pro Werktag innerhalb der EU 207 Millionen bargeldlose Retail-Zahlungen durchgeführt[2] – allerdings verlassen die meisten dieser Zahlungen (noch) nicht nationales Terrain. Die Elektronisierung beeinflusst die Strukturen des Marktes für Zahlungssystem-Dienstleistungen stark. Neue Anbieter und kreative Lösungsansätze haben diesen Markt entlang der Wertschöpfungskette verändert, von der reinen Daten- und Transaktionsebene bis hin zum Entstehen neuer Zahlungssystemanbieter. Entgegen dem noch vor zwei Jahrzehnten gängigen Konzept – Banken und ihre Tochterunternehmen bestimmen den Zahlungsverkehr – sind neue Marktteilnehmer unaufhaltsam in diesen Markt vorgedrungen: Internet Payment Service Provider, Telekommunikationsunternehmen, Systemhäuser, Softwareentwickler und andere, darunter vermehrt Nicht-Banken. Deren technisches Know-How, das sie im Zusammenhang mit der „digitalen Revolution“ gewonnen haben, unter anderem beim Aufbau und Betrieb von Rabattsystemen im Internet, der Entwicklung von Bonuskarten und der digitalen Verwertung von Rechten, nutzen sie nunmehr auf dem Markt für Zahlungssysteme. Krueger geht sogar noch einen Schritt weiter und postuliert, dass viele der Firmen, die in den obengenannten Gebieten erfahren sind, ebenso wie reine Technologieentwickler und -lieferanten potenzielle Zahlungssystemanbieter sind.[3]

Die skizzierten Veränderungen haben sowohl bei den Großzahlungen als auch bei den Massenzahlungen starke Einflüsse auf die Infrastrukturentwicklung und den Betrieb der Systeme. Der Markt für Großzahlungen in Europa zeichnet sich in den letzten Jahren durch hohen Wettbewerb und neue Systeme mit ungewohnt kurzen Innovationszyklen aus. Im Massenzahlungsverkehr wird bislang weniger die Infrastruktur selbst als vielmehr der Zugang zu dieser Infrastruktur berührt. Neue Zugangsprodukte über verschiedene multimediale Kanäle wie das Internet und das Mobiltelefon in verschiedenen Ausprägungen kennzeichnen die letzten Jahre mit neuen Zahlungsverfahren wie Scratch-Karten, Bezahlen mit Mobiltelefon

[1] Vgl. White (1997), S. 15 ff., der im Titel seines Aufsatzes die Entwicklung auf den Punkt bringt: “The Technology Revolution And Monetary Evolution.“
[2] EU (2003), EZB (2002d), S. 19f. Zu den bargeldlosen Zahlungsmitteln zählen bei dieser Rechnung: Schecks, Kredit- und Debitkartenzahlungen, Überweisungen, Lastschriften und (kartenbasierte) eGeld-Zahlungen.
[3] Vgl. Krueger (2001), S. 9.

und Online-Überweisung. Es werden aber auch beim Massenzahlungsverkehr durch die zunehmend zeitnahe Verarbeitung von Zahlungsaufträgen Veränderungen bei der Infrastruktur erwartet.

Die volkswirtschaftliche Bedeutung des Zahlungsverkehrs ist offensichtlich: 2002 wurden an den 255 Arbeitstagen des größten europäischen Zahlungssystems TARGET 64,5 Mio. Zahlungen bearbeitet mit einem Gegenwert von € 395 Billiarden, das heißt allein TARGET wälzt ungefähr alle sechs Arbeitstage das jährliche Bruttoinlandsprodukt der EU-15 einmal um.[4] Dies erfordert besonders hohe Sicherheitsvorkehrungen. Insbesondere der informationstechnologische Wandel, der den weltweiten Einsatz offener Netze stark vorangetrieben hat, lässt neue Ansätze zur Bestimmung und Überprüfung der Sicherheit im Zahlungsverkehr notwendig erscheinen; die bisherigen Konzepte zur Gewährleistung von Sicherheit geraten auf den Prüfstand. Elektronische Angriffe auf bestehende Infrastrukturen haben eine andere Qualität als bisherige Vorfälle, die meist eine physische Präsenz der Angreifer erforderten. Die beeindruckenden Schadensfälle beim (Kredit-)Kartenbetrug im US-amerikanischen Markt belegen dies beispielhaft: Während beim stationären (Offline-)Einzelhandel die Betrugsquote 2002 bezogen auf die Transaktionszahl bei rund 0,07 Prozent lag, wurde im eCommerce mit 2,1 Prozent ein 30-mal höherer Wert erreicht.[5] Für Europa werden ähnliche Größenordnungen angenommen.[6]

Konsultationen auf internationaler Ebene haben erst kürzlich zu einer Neuen Basler Eigenkapitalvereinbarung (Basel II) geführt. Dort bekommen Operationelle Risiken, zu denen auch informationstechnologische und organisatorische Risiken gehören, einen eigenen Stellenwert. Sie sollen ab dem Jahr 2006 mit Eigenkapital unterlegt werden. Mit der europäischen Währungsunion und Erweiterung geht ferner ein Umbau bisheriger aufsichtlicher Strukturen im Finanzsektor einher, der die Frage einer bedarfs- und zielgerechten Aufgabenteilung innerhalb des Europäischen Systems der Zentralbanken (ESZB) mit sich bringt.

Die zentrale Frage der vorliegenden Arbeit lautet, wie in diesem Umfeld die Sicherheit des elektronischen Zahlungsverkehrs in Deutschland mit Hilfe der existierenden Regel- und Kontrollstrukturen sowie bei gegebener Marktstruktur und -entwicklung gewährleistet werden kann. Kernelement der Analyse ist neben der Untersuchung der bislang nur in Fragmenten diskutierten Frage, inwieweit bisher Zahlungsverkehrssicherheit überhaupt reguliert wird, die mögliche Ausgestaltung des regulatorischen Rahmens. Regulierung meint in diesem Zusammenhang nicht allein staatliches Regulieren, sondern umfasst ebenso privatwirtschaftliche Initiativen sowie Standardisierungsgremien und -organisationen.

Barvell bringt die Schwierigkeiten der Legislative und der Regulatoren, die in dieser Arbeit behandelt werden sollen, auf den Punkt:[7] „It could be debated which one of the models would be the best one to choose. If we purely look at the need for the payment system, one has to keep in mind that the payment system is under constant development, and that we do not know today, what kind of new developments we will see tomorrow. Nevertheless, I believe that the payment system market would benefit from a regulatory framework that includes less precise regulation in the form of a law, giving the overseer the power to regulate the system more in detail. This is not to say that there cannot be situations where a more detailed regulation has to be included in the law, but this should rather be the exception than the rule.“

[4] Zahlen zu TARGET aus EZB (2003c), S. 6 und EZB (2003e), S. 4. BIP der EU-15 im Jahr 2002:
€ 9.170,13 Mrd. (gerechnet in jeweiligen Preisen) (SVR (2003), Tabelle 3*, S. 501).
[5] Vgl. Pago (2003), S. 133.
[6] Vgl. KOM (2001).
[7] Barvell (2002), S. 21.

1.2 Aufbau der Arbeit

Die Arbeit gliedert sich in drei Hauptteile. In einem ersten Teil werden die Grundlagen dargelegt und bereits mit Bezug zur Sicherheitsthematik (Kapitel 2 und 3), die Zahlungsverkehrslandschaft in Deutschland, die verschiedenen Akteure und die Schnittstellen zu europäischen wie internationalen Systemen aufgezeigt. Groß- und Massenzahlungssysteme werden dabei getrennt dargestellt.

Der Finanzsektor ist in Deutschland ein seit Jahrzehnten hoch regulierter Bereich, der mit einigen Ausnahmeregelungen, beispielsweise im Kartellrecht, ausgestattet ist. Schadensfälle wie die Insolvenz der Herstatt-Bank haben in der Folge jeweils zu ergänzenden Auflagen geführt. Das Thema Sicherheit der Informationstechnologie und Zahlungsverkehr war nicht im Fokus regulatorischer Bemühungen. Erst mit der Jahr 2000 Umstellung und dem Anschlag auf das World Trade Center am 11.09.2001 ist die Bedeutung kritischer Infrastrukturen und ihre systematische Untersuchung in vielen Wirtschaftszweigen vermehrt thematisiert worden.

Das regulatorische Umfeld im Bereich des elektronischen Zahlungsverkehrs ist historisch gewachsen und dementsprechend komplex. Die Arbeit zeichnet die einzelnen Institutionen nach, die von nationaler bis internationaler Ebene Einfluss auf die Bestimmungen zur Sicherheit im Zahlungsverkehr nehmen. Es wird gezeigt, dass der Großzahlungsverkehr in Bezug auf Sicherheitsfragestellungen deutlich reglementierter und überschaubarer ist als der Massenzahlungsverkehr. Die erwähnten Trends lassen jedoch in Zukunft auch den Massenzahlungsverkehr vermehrt zum Gegenstand aufsichtsrechtlicher Überlegungen werden (Kapitel 4).

Der zweite Hauptteil der Untersuchung geht in Kapitel 5 der Frage nach, welche besonderen Risiken im Zahlungsverkehr auftreten, und welche Regulierungen in diesem Zusammenhang bereits existieren. Dies geschieht anhand der im ersten Teil aufgeführten Institutionen und mit besonderem Schwerpunkt auf den Arbeiten der Bank für Internationalen Zahlungsausgleich im Rahmen von Basel II über den Umgang und das Management Operationeller Risiken. Für das Jahr 2001 ergab eine Umfrage der Bank für Internationalen Zahlungsausgleich (BIZ) unter 89 Banken Schäden durch Operationelle Risiken in Höhe von € 7,8 Mrd.[8] Zwar ist lediglich ein Teil dieser Schadenssumme im Zahlungsverkehr entstanden, im Zahlungsverkehr allerdings ist das Management Operationeller Risiken von großer Bedeutung. Zahlungssysteme sind selten klassischen bankbetrieblichen Risiken ausgesetzt (Adressausfallrisiko, Zinsänderungsrisiko etc.), vielmehr sind Schäden, die beim Betrieb von Zahlungssystemen entstehen, größtenteils Operationellen Risiken zuzuordnen. Allein im Bereich Zahlungskartenbetrug innerhalb der Europäischen Union wurde 2001 der Schaden auf € 600 Mio. geschätzt – dies entspricht einer Steigerung um 50 % gegenüber dem Vorjahr.[9] Basierend auf den Vorschlägen der BIZ wird am Beispiel Operationeller Risiken im elektronischen Zahlungsverkehr ein erweiterter Ansatz zur Risikoidentifizierung und -bewältigung vorgestellt.

Im letzten Teil der Arbeit (Kapitel 6) wird darauf aufbauend mit dem „Rautenmodell“ der Regulierung ein Modellrahmen dargestellt, mit dessen Hilfe regulatorische Vorgehensweisen beurteilt werden können. Es kann gezeigt werden, dass ein realisierbares Aufsichts-Regime in diesem Problemkreis nicht ausschließlich auf quantitativen Entscheidungsgrundlagen basieren kann, sondern zum großen Teil in der Lage sein muss, qualitative Argumente verarbeiten zu

[8] BIZ (2003f), S. 10, Tabelle 6, Panel A. In den Erhebungszeitraum fallen auch die Terrorschäden durch den Anschlag am 11.09.2001.
[9] KOM (2001).

können. Die Entscheidung, welches aufsichtliche Konstrukt letztlich geeignet ist, mit den Herausforderungen der technologischen Entwicklung umzugehen, erweist sich als in letzter Instanz politisch, da die Präferenzen innerhalb des vorgestellten Rautenmodells der Regulierung nicht wertneutral getroffen werden können. Kapitel 7 zieht ein Fazit der Untersuchung und gibt einen Ausblick auf die zukünftigen Entwicklungen im Bereich sicheren elektronischen Zahlungsverkehrs.

1.3 Angestrebte Ergebnisse der Untersuchung

In der vorliegenden Arbeit werden elektronische Zahlungssysteme unter dem Gesichtspunkt der Sicherheit umfassend dargelegt. Die Diskussion der Risiken, insbesondere der Operationellen Risiken, verdeutlicht die Herausforderung, der sich die Finanzwelt bei einem vermehrten Einsatz von Informationstechnologie in Zukunft stellen muss.

Zur Zeit ist der elektronische Massenzahlungsverkehr sowohl in den USA als auch in Europa, aus unterschiedlichen Gründen, noch nicht so stark entwickelt wie der Großzahlungsverkehr. Aufgrund der großen Volumina bei geringen Einzelwerten ist der Aspekt der Überwachung der Sicherheit im Massenzahlungsverkehr bislang nicht stark betont. Die Zentralbanken sehen sich zunächst in der Rolle des Katalysators. Erste öffentliche Konferenzen, Arbeiten und Konsultationen verdeutlichen aber, dass die Ausgestaltung der Sicherheit dieser Systeme zunehmend eine Rolle spielt. Anhand der Vorschläge, die bei den Fortgeschrittenen Verfahren zum Management Operationeller Risiken für Basel II diskutiert werden, wird ein erweiterter Ansatz entwickelt, der die Zusammenarbeit von Aufsicht und Kreditinstituten national wie international zumindest im Bereich Zahlungsverkehr im Sinne des bei Basel II angestrebten Supervisory Review Processes intensivieren würde. Ein klarer Vorteil dieses Vorgehens liegt in einer möglichen Verbesserung der Sicherheit im Zahlungsverkehr. Mit dem vorgestellten Ansatz könnten die Kreditinstitute einen erkennbaren Nutzen aus der von der Aufsicht vorgeschriebenen Regulierung erzielen, ohne wettbewerbsverzerrende Nebeneffekte befürchten zu müssen.

In der Arbeit wird ferner gezeigt, wie ein privatwirtschaftliches und staatliches (inklusive Mischformen) regulatorisches Regime in Zukunft „idealerweise“ aussehen könnte, mit dem die Herausforderungen der neuen (Informations-)Technologien und ihrer Bedrohungen wirksam bewältigt werden können. Erst im Anschluss an eine klare Zielbestimmung regulatorischer Eingriffe kann festgelegt werden, welche Institution auf welcher Ebene mit welchen Aufgaben betraut werden soll und kann.

In der vorliegenden Untersuchung soll die Bedeutung kooperativen Handelns zur Gewährleistung der Sicherheit in elektronischen Bezahlsystemen deutlich herausgearbeitet werden. Stärker als bisher müssen sich die Marktteilnehmer und die Aufsichtsbehörden aufeinander einstellen und miteinander Konzepte und Regularien zur Gewährleistung festgelegter Sicherheitsniveaus erarbeiten. Die zunehmende Komplexität global vernetzter Zahlungssysteminfrastrukturen erfordert eine Betonung qualitativer Aspekte der Sicherheit und Regulierung. Gleichwohl bleibt das Ziel einer quantitativen Untermauerung der qualitativen Vorgaben bestehen. Die Formalisierung und vor allem die Meßbarkeit qualitativer Sicherheitsaspekte kann jedoch nur in Kooperation von Regulatoren und Marktteilnehmern im nötigen Umfang erreicht werden. Neben einer zunehmenden Europäisierung und Internationalisierung werden dabei neue Akzente bei der institutionellen Zusammenarbeit erforderlich. Erste Ansätze in diese Richtung zeigen die jüngsten Aktivitäten der Bundesanstalt für Finanzdienstleistungsaufsicht auf nationaler und der Europäischen Zentralbank auf europäischer Ebene.

2 Sicherheit im Zahlungsverkehr und Regulierung: Begriffsbestimmungen

„It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machine and its terminals in a shielded room, and post a guard at the door.“[10]

2.1 Spannungsfeld: Risiko und Sicherheit

Der nachhaltige Erfolg der zunehmenden Elektronisierung unserer Gesellschaft im Allgemeinen und des Zahlungsverkehrs im Besonderen hängt wesentlich vom Vertrauen in die Sicherheit und Zuverlässigkeit der eingesetzten Medien ab, auch als eTrust bezeichnet.[11] Sind bei reinen Kommunikationsdiensten wie beispielsweise eMail höchstens die Schnelligkeit der Informationsübertragung und gewisse Datenschutzaspekte relevant, so sind bei nicht funktionierenden Zahlungssystemen monetäre Interessen berührt.

Der Einsatz elektronischer Zahlungssysteme setzt voraus, dass die Anwender sowohl im Retail- als auch im Großzahlungsverkehr die Funktionalität, Stabilität, Robustheit gegen Angriffe, Haftungsfragen im Falle eines nicht selbst zu verantwortenden Problems etc. so beurteilen, dass sie die Systeme trotzdem verwenden oder sogar in verstärktem Maße auf diese zurückgreifen. Mit den damit verbundenen Schwierigkeiten haben neben den Konsumenten und Händlern, der Aufsicht und den Systementwicklern auch die Betreiber von Bezahlsystemen zu kämpfen. Die Koordination von Aufgaben und Verantwortlichkeiten im weltweiten Datennetz ist diffizil, die Rechtsgrundlage und -gültigkeit von elektronischen Geschäften ist international weit davon entfernt, einheitlich zu sein. Hinzu kommt, dass eTrust nur entstehen kann, falls die Geschäftspartner bei elektronischen Geschäften der Überzeugung sind, die zugrundeliegende Technik zu beherrschen. Ist schon der Erklärungs- und Schulungsbedarf, um die Systeme bei den potenziellen Anwendern zum Laufen zu bringen, prohibitiv hoch, kann von eTrust keine Rede mehr sein. Diese Erfahrung mussten beispielweise die Entwickler der sicheren Kreditkartenzahlung via Secure Electronic Transaction (SET) machen. Die Komplexität von SET gekoppelt mit fehlender Akzeptanz führte mittlerweile zur Entwicklung modifizierter Technologien („MasterCard Secure Code“ und „Verified by Visa“), die im Markt erst neu positioniert werden müssen.

Ein weiteres Problem bei der Gestaltung und Nutzung komplexer Technologien ist die Kostenübernahme: Wer trägt die Kosten und wer profitiert in welchem Maß von einer neuen Technologie, z. B. von sicheren Kreditkartenzahlungen mittels Chip? So kann der zögerliche Einsatz der digitalen Signatur, trotz vergleichsweise schneller legislativer Reaktion, allein durch diese Schwierigkeit erklärt werden. Die ungelöste Frage der Kostenübernahme ließ nach dem Scheitern privatwirtschaftlicher Initiativen im Bereich digitaler Signaturen den Ruf nach Public-Private-Partnership laut werden.

Sicherheit elektronischer Zahlungssysteme im Sinne einer vollständigen Garantie, ohne Schadensfälle und Geschädigte, gibt es nicht. Für den weiteren Entwicklungspfad der Elektronisierung ist die Ausgestaltung des ‚Spielfelds' entscheidend, in dem sich die jeweiligen Aktivitäten abspielen. Für den Zahlungsverkehr bedeutet dies, dass die aufsichtlichen Rahmenbedingungen mit der technologischen Entwicklung Schritt halten müssen. Insbesondere sollten die Risiken, denen elektronischer Zahlungsverkehr ausgesetzt ist, von den verantwortlichen Akteuren auch in Zukunft so beherrscht werden, dass einerseits

[10] Cheswick (1994), zitiert in Palensky et al. (2000), S. 31.
[11] Vgl. HVB(2001), S. 12 f.

auftretende Schadensfälle im System nicht überproportional zunehmen können, andererseits die Verteilung der entstehenden Kosten und Schäden im Konsens mit allen beteiligten Akteuren geschieht.

Den Ansprüchen an Sicherheit in elektronischen Zahlungsverkehrssystemen kann nur gerecht werden, wer die verschiedenen im folgenden aufgezeigten Ebenen der Sicherheit und die Interessen der beteiligten Akteure adäquat berücksichtigt. Ein geeigneter Risiko-Management-Prozess, der die Identifikation und Bewertung der Risiken sicherstellt, die Maßnahmen zum Umgang mit den identifizierten Risiken festlegt und den Kontroll- und Prüfzyklus bestimmt, steht im Kern einer solchen Aktivität. Auf Seiten der Aufsicht ist zu prüfen, inwieweit der Markt für Finanzdienstleistungen den gewünschten Prozess selbst in Gang bringt und wie viel hoheitliche ‚Katalysatorfunktion' noch notwendig erscheint. Der technologische Fortschritt, der sich u. a. in der zunehmenden Elektronisierung des Zahlungsverkehrs niederschlägt, lässt neuartige Verfahren des Risikomanagements notwendig erscheinen.

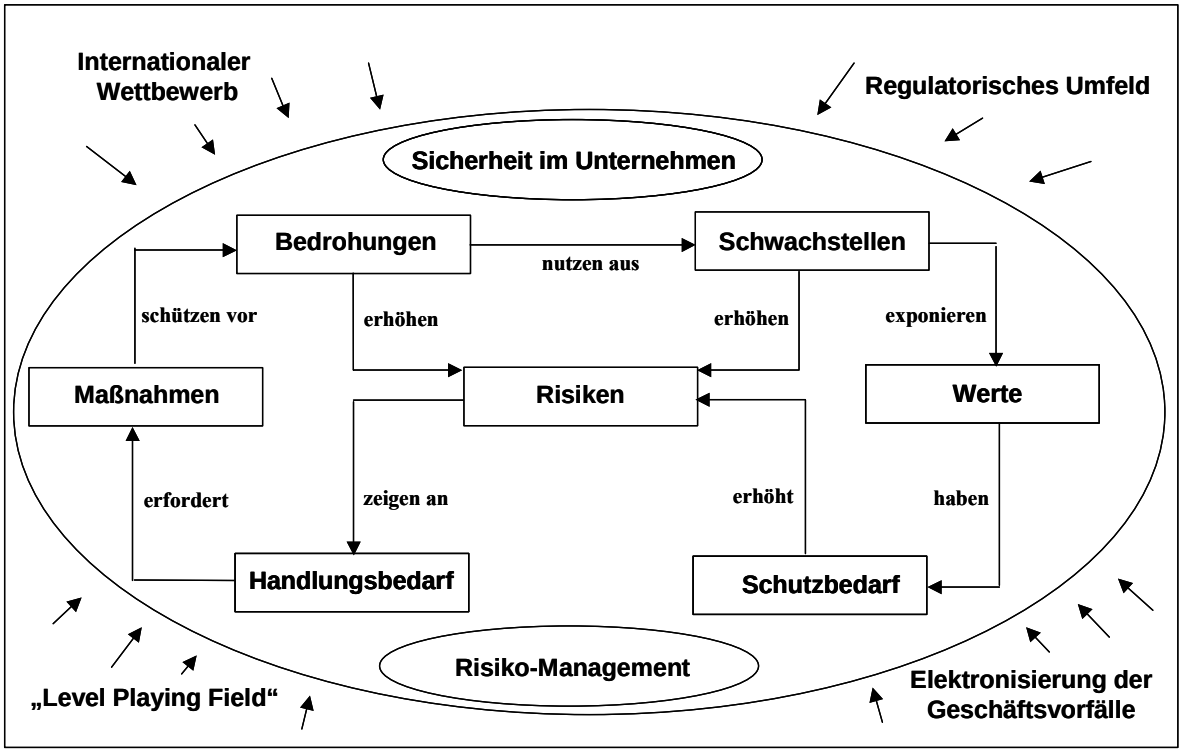

Abbildung 1: Wirkungszusammenhänge des Risikomanagements im Unternehmen[12]

[12] In Anlehnung an Plate (1999).

Die Finanzwelt kann, so zeigt die Analyse, auf bewährte Konzepte des Risikomanagements zurückgreifen. Die Komplexität der Aufgabe (siehe Abbildung 1) ist jedoch mittlerweile so hoch, dass jede Branche ihre eigenen Regeln und Verfahren ausdifferenzieren muss. Die regulatorischen Bemühungen, banktypische Risiken im Allgemeinen und Operationelle Risiken im Besonderen zu minimieren, wurden in den letzten Jahren verstärkt. Abbildung 1 verdeutlicht die Wirkzusammenhänge, in denen Risikomanagement im Unternehmen gesehen werden muss. Risiken im Zahlungsverkehr bedrohen die Sicherheit des Unternehmens, Bedrohungen, die Schwachstellen ausnutzen, erhöhen diese Risiken. Das Risikomanagement, ausgehend von schutzbedürftigen Werten, erkennt nötigen Handlungs- und Schutzbedarf und setzt die als geeignet identifizieren Maßnahmen um. Dabei ist das Unternehmen neben dem internationalen Wettbewerb und der zunehmenden Digitalisierung der Geschäftsprozesse dem regulatorischen Umfeld ausgesetzt. Im europäischen Kontext spielt im Zahlungsverkehr zunehmend der Gedanke eines einheitlichen „Level Playing Fields“ der Regulierung eine wichtige Rolle für die entsprechende Positionierung des Unternehmens im Wettbewerb.

2.2 Risikobegriff

Unsicherheit teilt sich auf in Ungewissheit und Risiko. Risiko ist gekennzeichnet durch subjektiv oder objektiv berechenbare aber auch bereits bekannte Eintrittswahrscheinlichkeiten. Bei Ungewissheit ist die Wahrscheinlichkeit für das Eintreten relevanter Umfeldeinflüsse unbekannt.

Risiko kann definiert werden als „Ausdruck für die Gefahr, dass das effektive Ergebnis vom gewünschten oder geplanten negativ abweicht“[13]; im Fall einer positiven Abweichung wird von Chance gesprochen. Aus bankbetrieblicher Sicht ist bedeutsam, dass Risiken nicht nur finanzielle Einbußen bedeuten, und somit vermieden werden müssen, sondern auch ein wesentlicher Bestandteil der Finanzintermediation sind. Wenn die erwarteten Verluste aus eingetretenen Risiken höher sind als die einkalkulierten, wird dies finanziell im Ergebnis sichtbar. Beispielsweise wird im Kreditgeschäft das Adressausfallrisiko in die Konditionen für die Vergabe von Krediten eingerechnet, und nur bei anteils- oder volumenmäßig höheren als den geschätzten Ausfällen wird die festgelegte Zielgröße negativ verfehlt. Risiko im Sinne bankaufsichtlicher Interpretation ist die Möglichkeit einer solchen negativen Ergebnisentwicklung.

Aus bankbetrieblicher Sicht gibt es verschiedene Ausprägungen von Risiko, denen nicht nur die Unternehmung selbst sondern auch die Regulierer mit angemessenen Maßnahmen begegnen wollen und müssen. Seit jeher sind sowohl Kreditrisiken, und das in dieser Kategorie bekannteste Risiko, das Adressausfallrisiko, als auch die Marktrisiken Gegenstand der Regulierung. Strategischen Risiken hingegen kann nur schwer mit einer aufsichtsrechtlichen Gestaltung begegnet werden, auch wenn sie sicherlich von entscheidender Bedeutung für den Fortbestand eines Unternehmens sein können. Operationelle Risiken sind bis Ende der neunziger Jahre weitgehend von Regulierungsbemühungen, aber auch bankinterner systematischer, das heißt einheitlicher, Erfassung verschont geblieben. Im Idealfall wären die Unternehmensziele und die der Regulierer deckungsgleich, Regulierung könnte minimiert werden. Insbesondere die unterschiedliche Beurteilung von Risiken jedoch, und zusätzlich die Möglichkeit krimineller Handlungen, erfordern unter der Annahme schutzbedürftiger Kleinanleger Regulierungsaktivitäten.
Die Klassifikation von bankbetrieblichen Risiken ist in der Literatur je nach Blickwinkel verschieden. Während Büschgen die Geschäftsrisiken in Ausfall- und Preisrisiken unterteilt, wird bei der Bank für Internationalen Zahlungsausgleich in Markt-, Kreditrisiken und

[13] Geiger (1999), S. 556.

Operationelle Risiken unterteilt.[14] Die sogenannten „Anderen Risiken“ werden bei Büschgen lediglich in Form von Betriebsrisiken als Risiken im internen Leistungsbereich erwähnt.[15] Jede gewählte Einteilung, die in mehrere Unterkategorien klassifiziert, erzeugt angesichts der Vielfalt verschiedener Risiken Überschneidungen und unklare Zuordnungen.

Operationelle Risiken gemäß Abbildung 2 lassen sich zunächst von anderen banktypischen – und vielfach weitaus geläufigeren und modelltechnisch erfassten – Risiken abgrenzen und weiter unterteilen.

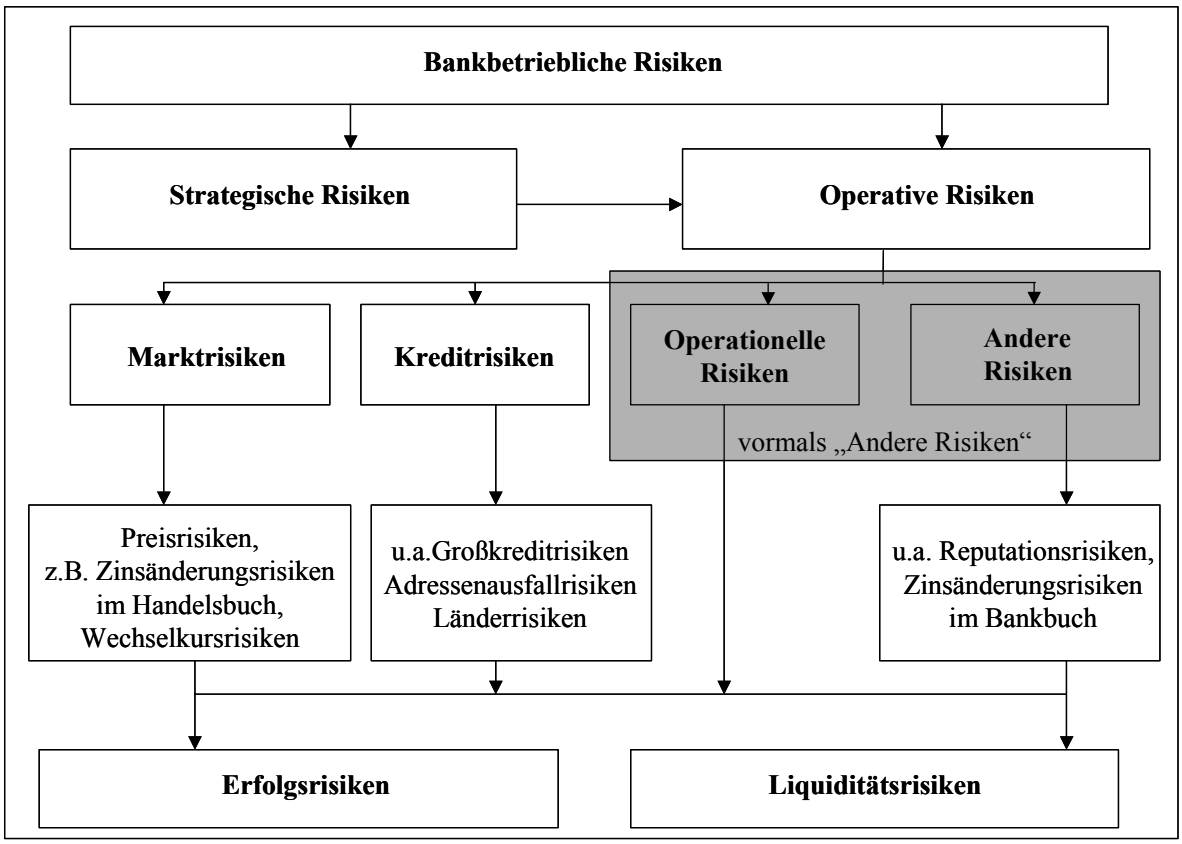

Abbildung 2: Systematik bankbetrieblicher Risiken[16]

Neben dem Begriff Operationelle Risiken (aus dem Englischen „operational risk“), der in dieser Arbeit vorwiegend verwendet wird, findet sich synonym auch „Operationale Risiken“. Nicht nur der Begriff variiert im deutschen Sprachgebrauch, es gibt auch keine allgemein anerkannte Standarddefinition.

In einer ersten Bestandsaufnahme und dem Versuch einer Begriffsfestlegung stellte das Basler Komitee für Bankenaufsicht 1998 fest, dass unterschiedlichste Definitionen Operationeller Risiken existieren, je nach befragter Institution. Operationelle Risiken beinhalten im Verständnis der Geschäftsbanken unter anderem die Risiken im Bereich der Zahlungssystem-

[14] Vgl. Büschgen (1998), S. 870, BIZ (2001c), BIZ (1998a).
[15] Allerdings sei darauf hingewiesen, dass Büschgen (1998), S. 885 ff., bereits operative Risiken in Risiken personeller und technischer Art untergliedert und auch die Rechtsrisiken in diese Kategorie einstuft.
[16] Basierend auf Büschgen (1999), S. 870, BIZ (2001c), BIZ (1998c), Hofmann (2002b), S. 8 ff., Stickelmann (2002), S. 14 f., eigene Darstellung. Anmerkung: Handelsbuch und Anlagebuch werden nach § 1 Abs. 12 KWG, § 2 Abs. 11 KWG unterschieden. Das Bankbuch (banking book, Synonym: Anlagebuch) stellt dabei eine Residualgröße dar, für alle Geschäfte, die nicht im Handelsbuch aufgeführt werden müssen.

abwicklung und betriebliche Unterbrechungen, ferner neben administrativen auch rechtliche Risiken.[17]

Es gibt den Begriff „operational risk“ im Bankensektor schon seit Jahrzehnten, gleichwohl führte diese Risikoart eher ein Nischendasein. Im September 1997 wurden Operationelle Risiken jedoch in den „Core Principles for Effective Banking Supervision“ in die Kategorisierung der dort aufgeführten Risiken mit aufgenommen.[18] Die Bank für Internationalen Zahlungsausgleich forderte in einem Unterpunkt zum Thema Risikomanagement zu diesem Zeitpunkt bereits effektive interne Kontrollmechanismen und Audits und explizit ein Management Operationeller Risiken.[19]

Erst Ende der neunziger Jahre begann die Bankenaufsicht im Zuge der Vorarbeiten zu Basel II[20] auf supranationaler Ebene das Risikomanagement und den Umgang der Banken mit Operationellen Risiken zu untersuchen; fast zeitgleich mit der 6. Novelle des Kreditwesengesetzes (KWG) und dem neu eingefügten § 25 a und dem Ergänzungs- und Änderungsgesetz Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), in dem Aktiengesetz und Handelsgesetzbuch verschärft wurden.[21] Allerdings stellte der Basler Ausschuss für Bankenaufsicht noch im September 1998 fest – ein Jahr nach der Veröffentlichung der „Core Principles for Effective Banking Supervision“: „Most banks that are considering measuring operational risk are at a very early stage, with only a few having formal measurement systems and several others actively considering how to measure operational risk. The existing methodologies are relatively simple and experimental, although a few banks seem to have made considerable progress in developing more advanced techniques for allocating capital with regard to operational risk.“[22]

Im Januar 2001 wurde Operationelles Risiko von der Bank für Internationalen Zahlungsausgleich (BIZ) vorläufig definiert als: „the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.”[23] Die direkten und indirekten Verluste waren für eine handhabbare Definition noch zu weit gefasst und Abgrenzungsprobleme waren absehbar. Diese wurden mit einer Aufzählung gelöst, die relevante Risiken oder mögliche Ereignisse aufführt, die Verluste hervorrufen könnten. Für diese Kategorien müssen auf Seiten der Kreditinstitute Daten gesammelt, aufbereitet und weitergegeben werden.[24] Die BIZ hatte dabei von Anfang an die mögliche Quantifizierung der Operationellen Risiken im Auge, da nur in diesem Fall aufsichtliche Maßnahmen überprüft und verglichen werden können.[25] Aus Sicht der BIZ gilt für die Finanzbranche die Definition Operationeller Risiken des Basler Ausschuss für Bankenaufsicht, die seit September 2001 verwendet wird: „the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”[26] Diese Definition verzichtet auf die ohnehin kritische Unterscheidung zwischen direkten und indirekten Verlusten. Indirekte Verluste können kaum trennscharf zugeordnet werden und hätten in der Folge zu erheblichen Interpretationsspielräumen geführt.

[17] BIZ (1998c), S. 3.
[18] Vgl. BIZ (1997), S. 22.
[19] Vgl. BIZ (1997), S. 28f.
[20] Siehe vertiefend 5.1.3.1.3.
[21] Vgl. BIZ (2001b eng.) und EZB (1999b). Auch in früheren Arbeiten (z. B. BIZ (1994)) problematisiert die BIZ bereits Operationelle Risiken in bestimmten Geschäftsbereichen, beispielsweise bei Derivatgeschäften.
[22] BIZ (1998a), S. 3 f.
[23] BIZ (2001c), S. 2.
[24] Vgl. ausführlich Abschnitt 5.3.
[25] BIZ (2001i), S. 2 und S. 21 ff.
[26] BIZ (2001i), S. 2, BIZ (2003a), S. 2.

Alle Definitionen Operationeller Risiken schließen strategische Risiken und Reputationsrisiken aus, umfassen jedoch die resultierenden Rechtsrisiken. Gleichwohl geht das Basler Komitee davon aus, dass die Geschäftsbanken für ihre jeweiligen Zwecke durchaus verschiedene Definitionen Operationellen Risikos haben können. Wichtig ist für das Komitee, dass diese Definitionen die aus Sicht der BIZ wichtigsten substanziellen Risiken umfassen und in das jeweilige Risikomanagement Operationeller Risiken auf Institutsebene eingehen.[27] Insbesondere wird durch die „Sound Practices for the Management and Supervision of Operational Risk" keine zwingende Vorgabe einer Definition Operationeller Risiken auf Institutsebene gemacht. Als Anhaltspunkt für die Banken nennt das Komitee lediglich die wichtigsten Operationellen Risiken, die zu substanziellen Verlusten führen können, und die demzufolge Gegenstand des Risikomanagements sein müssen:[28]

- Interner Betrug, wie Diebstahl durch Mitarbeiter,
- Externer Betrug, wie Fälschungen, Angriffe auf Computersysteme,
- Risiken im Zusammenhang mit Beschäftigungspraktiken und Arbeitsplatzsicherheit, z. B. die Haftung bei Diskriminierung von Angestellten,
- Praktiken im Umgang mit Kunden, Produkten und Geschäftsgebaren, z. B. Verkauf unautorisierter Produkte, Geldwäsche,
- Beschädigung von Gütern, z. B. durch Vandalismus, Erdbeben, Terrorismus,
- Unterbrechung des Geschäfts und Systemversagen, z. B. bei Telekommunikationsproblemen, Software- und Hardwarefehlern,
- Probleme bei der Ausführung von Prozessen, wie etwa juristisch unvollständige Aufzeichnungen, Dateneingabefehler etc.

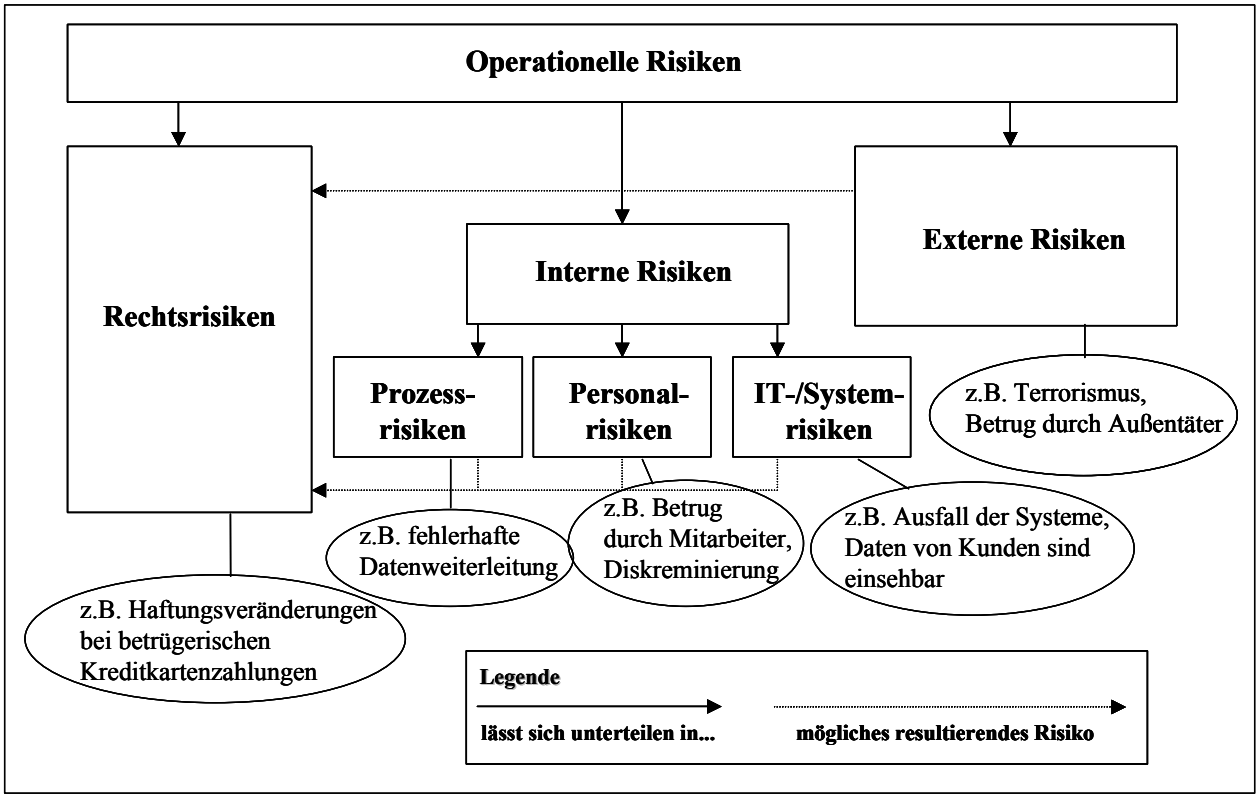

Abbildung 3: Arten Operationeller Risiken[29]

[27] Vgl. BIZ (2002e), S. 1.
[28] BIZ (2003a), S. 2.
[29] Nach Hofmann (2002), S. 8, BIZ (2003a), S. 2, Jörg (2002), S. 74, eigene Ergänzungen/Darstellung.

Zusammenfassend lassen sich Operationelle Risiken, gemäß Abbildung 3 unterteilen.

2.3 Sicherheitsbegriff

2.3.1 Sicherheit: Herleitung und Bedeutung

Der Begriff Sicherheit lässt sich etymologisch auf das lateinische „securitas“ zurückführen, bei den Römern die Gottheit der innen- wie außenpolitischen Sicherheit.[30] Während im deutschen Sprachraum der Begriff Sicherheit mit vielfältigsten Bedeutungen belegt ist, wird im englischsprachigen Raum deutlicher zwischen „safety“ und „security“ unterschieden:[31]

- „safety“: *Sicherheit als Zustand* im Sinne von Gefahrlosigkeit aber auch Sicherheit im Sinne der Zuverlässigkeit oder Verlässlichkeit eines Systems, Mechanismus oder Verfahrens. Schutz- und Sicherheitsvorrichtungen sind demzufolge „safety devices“, als Fremdwort im Deutschen augenfällig: der Safe.
- „security“: *Sicherheit* ebenfalls als Zustand aber auch *als Schutz(maßnahme)* im Sinne von ‚sicher vor’ oder ‚sicher gegen’ etwas sein (Gefahrenabwehr, „security against, from“). Security meint in diesem Verständnis auch die Werkspolizei und die Sicherheitsabteilung in einem Unternehmen. Ferner kann „security“ auch (innere) Sicherheit und Sorglosigkeit meinen. Darüber hinaus nimmt es im englischen Sprachraum auch die Bedeutung von Bürgschaft, Kaution und Bürge ein. Im Plural verwendet, bedeutet „securities“ Wertpapiere und verbriefte Sicherheiten.

Folgerichtig wird unter IT-Security das aktive Gestalten im Sinne von Schutzmaßnahmen der informationstechnologischen Sicherheit eines Unternehmens, Netzwerkes etc. verstanden.

Die verschiedenen Ausprägungen des Sicherheitsbedürfnisses und -verständnisses von Gesellschaften lassen sich aus sozialwissenschaftlicher Sicht über die gesamte Entwicklung der Menschheit beobachten. Grundsätzlich scheint die These empirische Unterstützung zu finden, der zufolge mit wachsender Zivilisationshöhe die Risikoakzeptanz einer Gesellschaft abnimmt, mithin also die Risikoaversion zunimmt.[32] Lübbe formuliert diesen Sachverhalt folgendermaßen:[33] „Das Sicherheitsverlangen wächst mit der Höhe des bereits erreichten technischen und sozialen Sicherheitsniveaus. Je sicherer wir leben, um so empfindlicher werden wir gegen Sicherheitseinbußen“. Gleichwohl können auch widersprüchliche Neigungen, wie das bewusste Eingehen von Risiken beispielsweise in der Freizeit oder im Straßenverkehr ausgelebt werden.

Sicherheit ist ein subjektives Bedürfnis und lässt sich kaum absolut festlegen. Auffallend bei den soziologisch motivierten Studien ist, dass der technische Sicherheitsbegriff in den Hintergrund tritt. Stapf verdeutlicht dies mit einer allerdings nicht repräsentativen empirischen Umfrage, bei der spontane Assoziationen zum Thema Sicherheit abgefragt wurden.[34] Die Ergebnisse lassen sich in der Reihenfolge der Erwähnungen gruppieren in die Felder „Private Sicherheit/persönlicher Bezug“, „Verkehrssicherheit“, „Öffentliche Sicherheit“, „Finanzielle bzw. ökonomische Sicherheit“ und eine Restkategorie. Technische Sicherheit in der Informationstechnologie kommt in diesem Zusammenhang nicht vor.

---

[30] Vgl. Stapf (1998), S. 51.
[31] Vgl. Langenscheidts Großes Wörterbuch Englisch-Deutsch, Stapf (1998), S. 52 f.
[32] Vgl. ausführlich Stapf (1998), S. 45 ff.
[33] Lübbe (1991): Die schwarze Wand der Zukunft, in: Fischer, E.P. (1991): Auf der Suche nach der verlorenen Sicherheit, Piper, München, Zürich, S. 17 – 31, S. 19 f. zitiert in Stapf (1998), S. 46.
[34] Stapf (1998), S. 53.

Sicherheit in der Informationstechnologie kann am ehesten in dem von Kaufmann in seiner umfassenden Kategorisierung verwendeten Begriff der Systemsicherheit eingeordnet werden.[35] Kaufmann versteht unter Systemsicherheit alle Sicherheit, die durch technische, juristische und ökonomische Mittel berechenbar hergestellt und vermittelt werden kann.

2.3.2 Informationssicherheit

Sicherheit kann bei Systemen, die vornehmlich auf Informationstechnologien basieren, zunächst mit Informationssicherheit gleichgesetzt werden. Informationssicherheit lässt sich von ihren grundlegenden Bedrohungen ausgehend betrachten. Vier Aspekte der Sicherheit können unterschieden werden, die eine mögliche Ausgangsposition für die Bewertung der Sicherheit eines Systems markieren. In dieser Sichtweise ist (Informations)sicherheit eines Systems dann vollständig gegeben, wenn:

1) Verfügbarkeit (availability),
2) Vertraulichkeit (confidentiality),
3) Integrität (integrity) und
4) Zurechenbarkeit

hergestellt und aufrecht erhalten werden können.[36]

ad 1) Verfügbarkeit bezeichnet die zugesicherte Eigenschaft eines IT-Systems, einen angebotenen Dienst in jedem Moment potenzieller Inanspruchnahme in gegebener Frist und erwarteter Qualität erbringen zu können. Ein System, welches die Verfügbarkeit eines Diensts oder einer Information garantiert, kann zu jedem Zeitpunkt den entsprechenden Dienst oder die Information ohne unzumutbare Wartezeit liefern.

ad 2) Vertraulichkeit einer Information oder eines Dienstes ist gewährleistet, wenn nur Personen sie lesen oder auf sie zugreifen können, die dazu befugt sind und deren Zugriff beabsichtigt war. Eine vertrauliche Nachricht beispielsweise darf nur von beabsichtigten Empfängern gelesen und interpretiert werden können. Die Vertraulichkeit der Identität eines Akteurs wird als Anonymität bezeichnet. Im Zusammenhang mit der Anonymität spielen die folgenden Begriffe eine Rolle:

- Pseudonymität (Abschwächung der Anonymität, z. B. Aliasse)
- Unverkettbarkeit (Informationen aus verschiedenen Aktionen lassen sich nicht zu neuen weiterführenden Informationen verknüpfen)
- Unbeobachtbarkeit (Existenz eines Kommunikationsvorgangs wird geheim gehalten).

ad 3) Integrität ist die zugesicherte Eigenschaft einer Nachricht, diese unverändert empfangen zu können. Der Inhalt der empfangenen Nachricht ist gleich dem Inhalt der gesendeten Nachricht. Veränderungen einer Nachricht können durch fehlerhafte Übertragung oder durch bewusste Aktionen eines Angreifers entstehen.

ad 4) Zurechenbarkeit bedeutet, dass der Verantwortliche für eine Nachricht oder Aktion zweifelsfrei festgestellt werden kann. Zurechenbarkeit von Nachrichten kann erreicht werden, wenn die Authentizität der Nachricht beweisbar ist. Authentizität ist dann gegeben, wenn eine Nachricht tatsächlich vom angegebenen Sender stammt. Der Begriff der Authentisierung und Identifizierung wird unter dem Schlagwort Authentifizierung zusammengefasst. Gelingt die

[35] Vgl. ausführlich Stapf (1998), S. 60 ff.
[36] Die Ausführungen basieren auf Röhm (2000), S. 18ff.

Authentifizierung ist die Rechtsverbindlichkeit von getroffenen Vereinbarungen ableitbar. Hierzu müssen auch die rechtlichen Rahmenbedingungen gegeben sein, die eine Beweisführung mit elektronischen Nachrichten vorsehen.[37]

Ein weiterer Aspekt der Sicherheit ist Fairness. Starke Fairness bezeichnet die Eigenschaft einer Folge von *k* Kommunikationsschritten zwischen *n* Parteien, dass entweder alle *n* Parteien alle *k* Nachrichten erhalten, die sie zurecht erwarten, oder keiner etwas erhält. Schwache Fairness bedeutet bei einer Folge von *k* Kommunikationsschritten, dass entweder alle Akteure die Nachricht erhalten, die sie zurecht erwarten oder andernfalls die Rechtmäßigkeit offener Forderungen einer dritten Partei nachgewiesen werden kann. Bei der starken Bedeutung, die Vertrauen für das Funktionieren von Zahlungsmitteln und Zahlungssystemen hat, ist die Eigenschaft der Fairness in der Regel bei der Überprüfung dieser Systeme zu gewährleisten. Beispielsweise ist es für Empfänger und Absender einer Zahlung von entscheidender Bedeutung, dass beide die gleiche Nachricht über den Erfolg oder Misserfolg einer Zahlungstransaktion erhalten. Wird diese Eigenschaft von einem Verfahren nicht in der Regel garantiert, werden sich alternative Systeme durchsetzen.

IT-Sicherheit kann also zunächst durch Verfügbarkeit, Vertraulichkeit, Integrität, Zurechenbarkeit und unter Umständen zusätzlich Fairness charakterisiert werden. In betriebswirtschaftlichen Abläufen ist die Konzentration auf IT-Sicherheit nicht ausreichend und hat in der Folge in den neunziger Jahren zu einer Erweiterung des Sicherheitsbegriffs geführt.

2.3.3 Mehrseitige Sicherheit und erweiterter Sicherheitsbegriff

Bedrohungen für die Sicherheit von Systemen in offenen Netzen haben im Vergleich mit „herkömmlichen“ Bedrohungen aus drei Gründen eine neue Dimension:

- die Automatisierung der Angriffe lässt Erfolge wahrscheinlicher werden,
- Handeln wird auf Distanz möglich,
- der Verbreitungsgrad und die -geschwindigkeit von Techniken, Informationen und Angriffen sind ungleich schneller geworden.

Grundlage für den im folgenden zugrunde gelegten Sicherheitsbegriff ist neben dem von Müller, Pfitzmann und anderen[38] entwickelten Ansatz der multilateralen, das heißt mehrseitigen, Sicherheit, respektive dualen Sicherheit, ein erweiterter Sicherheitsbegriff, der im Schalenmodell seinen Niederschlag findet[39].

Was bedeutet duale Sicherheit? Beim rein technischen Sicherheitsbegriff wird sehr viel Wert auf die Abläufe und Funktionalitäten gelegt. Das IT-System wird im althergebrachten Sinn meist losgelöst von seiner Einsatzumgebung betrachtet. In der dualen Betrachtung hingegen spielt der Mensch als Systemkomponente, also als Teil einer Funktionseinheit (z. B. PC, Netz, Webserver) eine bedeutende Rolle. Im folgenden wird nicht nur mit der rein technischen Auslegung des Sicherheitsbegriffs gearbeitet, sondern auch die Auswirkung auf die Nutzung der Informationstechnik betrachtet. Dies gilt einmal für den einzelnen Anwender aber auch für das Umfeld.

[37] Wie z. B. durch die Europäische Union in den letzten Jahren geschehen, vgl. hierzu Europäische Gemeinschaften (2000a) und Europäische Gemeinschaften (2000b).
[38] Vgl. Müller (1997) und Müller (1998).
[39] Vgl. Hartmann (2000), S. 151 ff und Zoche (1998).

An dieser Stelle setzt der Begriff der mehrseitigen Sicherheit an, der als Erweiterung des dualen Ansatzes verstanden werden kann. Sicherheit wird im Geschäftsprozess von verschiedenen Akteuren gefordert: Hersteller, Benutzer, Systembetreiber, Dienstleister und Aufsichtsorgane. Deren Ziele sind in Bezug auf Sicherheit nicht zwangsläufig deckungsgleich, daher muss IT-Sicherheit von mehreren (Akteurs-)Seiten beleuchtet werden.

Beim Einsatz von Informationstechnologie kann mehrseitige Sicherheit am Erfolg der Durchsetzbarkeit der oben genannten Schutzziele, Verfügbarkeit, Vertraulichkeit, Integrität, Zurechenbarkeit und Anonymität gegenüber (technisch versierten) Angreifern jeder Art gemessen werden.

Eine weitere Dimension des mehrseitigen Sicherheitsbegriffs ist die Subjektivität[40]: „Mehrseitige Sicherheit beschreibt einen technisch/organisatorischen Zustand der realisierten Kommunikationswege derart, dass das subjektiv wahrgenommene Sicherheitsbedürfnis von den Betroffenen selbstverantwortlich formuliert und die Durchsetzung ihrer Interessen gesichert werden kann.“ Spätestens an dieser Stelle wird deutlich, dass die rein technischen Sphären verlassen werden; Sicherheit kann nicht nur technisch gewährleistet werden. Die Schwierigkeiten mit einer objektiven Erfassung von Risiko und dessen subjektiver Wahrnehmung bringen normative Fragestellungen mit sich, die Stapf auf den Punkt bringt:[41] „How safe is safe enough?“

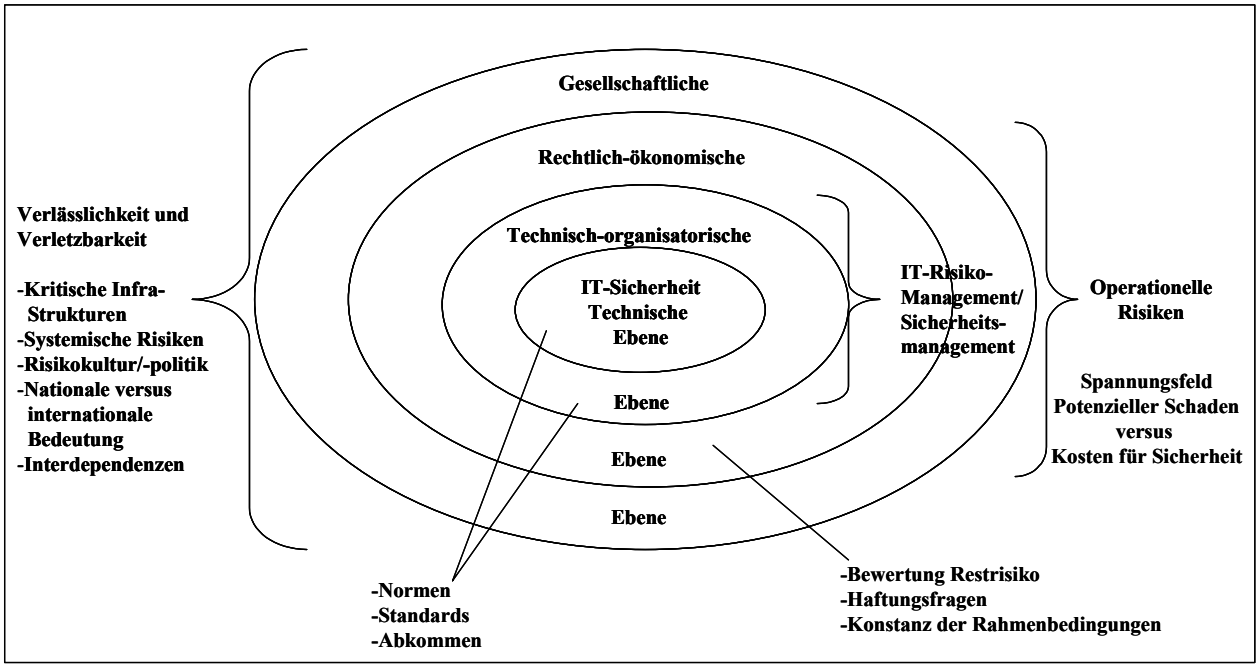

Abbildung 4: Der erweiterte Sicherheitsbegriff im Zahlungsverkehr[42]

Im Zahlungsverkehr ist dies von besonderer Bedeutung, da hier die Interessen der an einer Transaktion beteiligten Parteien durchaus unterschiedlich sein können. Beispielsweise ist beim Einkauf über das Internet der Verbraucher bereits in dem Moment zufrieden, in dem er seine bestellte Ware erhalten hat. Er ist nicht automatisch daran interessiert, ob im Gegenzug Geld von seinem Konto zum Händlerkonto geflossen ist – im Extremfall betrügerischer Absichten kann er sogar unter Umständen einer erfolgten Lastschrift auch nach Erhalt der

[40] Müller (1997), S. 13.
[41] Stapf (1998), S. 65.
[42] In enger Anlehnung an Hartmann (2000), S. 151 und Zoche (1998).

(korrekten) Ware widersprechen. Die Institutionen über die Zahlungen abgewickelt werden, haben wieder andere Interessen: die Bank des Zahlungspflichtigen möchte möglichst spät das Geld aus ihrem Banknetz fließen lassen (im Fall der Überweisung), die Bank des Händlers das Geld möglichst schnell erhalten (im Fall der gezogenen Lastschrift); und jeder bei aus seiner Sicht maximaler Transaktionssicherheit. Sicherheit bedeutet für jeden Beteiligten etwas anderes, grundsätzlich ist jeder bestrebt, Risiko zu einem möglichst späten Zeitpunkt zu übernehmen und möglichst kurz zu tragen.

Das Schalenmodell (siehe Abbildung 4) konzentriert sich weniger auf die Interessen der einzelnen Parteien bei einer Transaktion – die indirekt auch im Schalenmodell durchscheinen – sondern setzt bei den verschiedenen Bezugsebenen von Sicherheit an. Sicherheit war lange Zeit ein auf IT-Sicherheit reduziertes Problem bei der Entwicklung elektronischer Netze und Bezahlvorgänge. Sicherheit in der Informationstechnik ist jedoch ungleich der Sicherheit in der Technik. Sicherheit kann nur erreicht werden, wenn der Weg dorthin als kontinuierlicher Prozess gesehen wird; eine Auffassung die mittlerweile von vielen Experten geteilt wird, in der praktischen Umsetzung jedoch auf erhebliche Schwierigkeiten stößt.[43]

Um im Bild zu bleiben: Erst in der zweiten Hälfte der neunziger Jahre wurden vermehrt die äußeren Schalen (Ebenen) der Sicherheit thematisiert. In komplexen technischen Systemen bekommt die Ausgestaltung technisch-organisatorischer und menschlich-organisatorischer Sicherheit einen eigenen Stellenwert. Die Bedeutung, die im Zuge der Konsultationen zu Basel II dem Operationellen Risiko zugemessen wird, zeigt, dass das ‚Denken im Schalenmodell' das Risikomanagement der nächsten Jahre maßgeblich beeinflussen wird.

Die rechtlich-ökonomische Ebene hat im Zuge technischer Entwicklungen und komplexer Systeme an Bedeutung gewonnen. Exemplarisch verdeutlichen die EU-Richtlinien[44] über elektronische Signaturen und über elektronischen Geschäftsverkehr die Wichtigkeit verlässlicher Rahmenbedingungen für die Entwicklung dieser Märkte, aber auch die vermehrten Anforderungen an alle Marktteilnehmer, sich rechtskonform zu verhalten.

Auf der gesellschaftlichen Betrachtungsebene findet sich zuvorderst die systemische Sicherheit von Zahlungssystemen. Geld kann erst durch das Vertrauen, das es selbst in verschiedenen Formen genießt oder durch den guten Ruf der jeweils ausgebenden Institutionen bei der Bevölkerung die Funktion als gesellschaftlich akzeptiertes Zahlungsmittel erfüllen. Das Vertrauen in die Wertbeständigkeit des Geldes einerseits (Inflationsdruck/ Wechselkursstabilität) und in die Sicherheit des Geldes andererseits ist eine wichtige Bedingung für Zahlungssysteme. Jegliche Zweifel an der systemischen Sicherheit des Geldes oder weiter gefasst an der Funktionsfähigkeit von Zahlungssystemen können gravierende volkswirtschaftliche Schäden nach sich ziehen.

2.3.4 Verständnis des Sicherheitsbegriffs in dieser Arbeit

Die Vielschichtigkeit des Begriffs ‚Sicherheit' wird im folgenden noch einmal kurz aufgezeigt. Alle Aspekte sind im Anschluss von Bedeutung, wenn die Sicherheit von elektronischen Zahlungssystemen untersucht wird. Der Schwerpunkt der vorliegenden Arbeit liegt dabei nicht so sehr auf den technischen Grundlagen und Eigenschaften von Systemen, sondern vielmehr in der Betonung der Komplexität des Sicherheitsbegriffs.

[43] Bruce Schneier gilt als einer der wesentlichen Verfechter des Prozessgedankens – und hat als Informatiker und IT-Security Consultant erst im Jahr 2000 angefangen, diesen Aspekt noch vor rein technischer Sicherheit zu betonen (vgl. Schneier (2000)).
[44] Vgl. Europäische Gemeinschaften (2000a), Europäische Gemeinschaften (2000b).

Sicherheit sollte von drei verschiedenen Sichtweisen aus analysiert werden:

1) Die elementaren Forderungen aus der Informationstechnologie, Sicherheit über die Einhaltung der vier oder fünf Teilaspekte Verfügbarkeit, Vertraulichkeit, Integrität, Zurechenbarkeit und Fairness zu realisieren, behalten insbesondere auf der technischen Ebene volle Gültigkeit.
2) Unterschiedliche Ebenen der Betrachtung von Sicherheit spiegeln die Bedeutungsvielfalt des Begriffs Sicherheit sehr anschaulich wider: von der technischen Stufe der IT-Sicherheit über technisch/menschlich-organisatorische und rechtlich-ökonomische Ebenen bis hin zur gesellschaftlichen Betrachtungsebene. Die Komplexität des Problems steigt dadurch jedoch erheblich.
3) Sicherheit hat für jeden an einem Geschäftsvorfall beteiligten Akteur möglicherweise eine unterschiedliche Bedeutung. Sicherheit im Zahlungsverkehr muss unterteilt und aus dem Standpunkt alle Akteure betrachtet werden; beim Zahlungsverkehr zumindest aus Sicht der Konsumenten, der Händler, der Zahlungssystembetreiber, der Banken, der technischen Dienstleister und Aufsichtsbehörden.

Sicherheit im Zahlungsverkehr basiert auf dem Verständnis von Sicherheit im obigen Sinne. Soll Sicherheit gewährleistet werden, kann sie nicht mehr als Produkt verstanden werden, das nachträglich hinzugefügt oder aktualisiert wird, sondern Sicherheit muss vielmehr, dem Ansatz von Bruce Schneier folgend, als Prozess betrachtet werden. In der Folge sollte darauf geachtet werden, welche Geschäftsebene bei einer Sicherheitsanalyse betroffen ist. So sind bestimmte organisatorische Merkmale – beispielsweise die Zugangskontrolle (physisch wie virtuell) – für den Gesamtprozess von Relevanz. Andere, wie zum Beispiel die Einhaltung bestimmter Service Level Agreements (Dienstleistungs-Vereinbarungen), sind lediglich für Teil- oder Einzelprozesse von Bedeutung.

2.4 Zahlungsverkehr: Begriffsbestimmung

Zahlungsverkehr bezeichnet die „Zahlungsvorgänge einer Unternehmung und privater Haushalte in der arbeitsteiligen Volkswirtschaft“.[45] Es kann nach Art der verwendeten Zahlungsmedien der Barzahlungsverkehr, der bargeldsparende Zahlungsverkehr und unbarer Zahlungsverkehr unterschieden werden.[46] In der vorliegenden Arbeit ist insbesondere der unbare Zahlungsverkehr, der beleglos über elektronische Netze – sowohl Interbanken-Netze als auch offene Netze wie das Internet – abgewickelt wird, der sogenannte elektronische Zahlungsverkehr, Gegenstand der Untersuchung.

Konzeptionell lassen sich Zahlungsvorgänge in drei unterschiedliche Vorgänge zerlegen (vgl. Abbildung 5):

1) Transaktion: der Prozess, der einen Zahlungsauftrag und –ausgleich anstößt und erforderlich macht. Die Höhe des Betrages bestimmt das verwendete Bezahlverfahren.
2) Clearing wird verstanden als: „Das Verfahren der Übermittlung, der Abstimmung und in einigen Fällen der Bestätigung von Zahlungsaufträgen vor dem Zahlungsausgleich; unter Umständen schließt es eine Aufrechnung der Zahlungen und die Ermittlung von Nettopositionen für den Zahlungsausgleich ein.“[47] In Deutschland gibt es multilaterale Clearing-Vereinbarungen mit allen beteiligten Akteuren.

[45] Gablers Wirtschaftslexikon, 12. Auflage, S. 2843.
[46] Vgl. Büschgen (1998), S. 414.
[47] BIZ (2001b deutsch), S. 90.

3) Settlement ist der nach dem Clearing stattfindende Prozess der Akzeptanz einer Zahlung und der anschließende Zahlungsausgleich. Großzahlungen werden ausschließlich über Zentralbankkonten abgerechnet, während der Clearingprozess in privaten Abwicklungsnetzen oder bei der Zentralbank stattfinden kann. Im Massenzahlungsverkehr kann das Settlement zwischen Privatorganisationen, Banken und anderen Dienstleistern erfolgen, oder über die Zentralbank; nur in letzterem Fall ist Zentralbankgeld involviert.

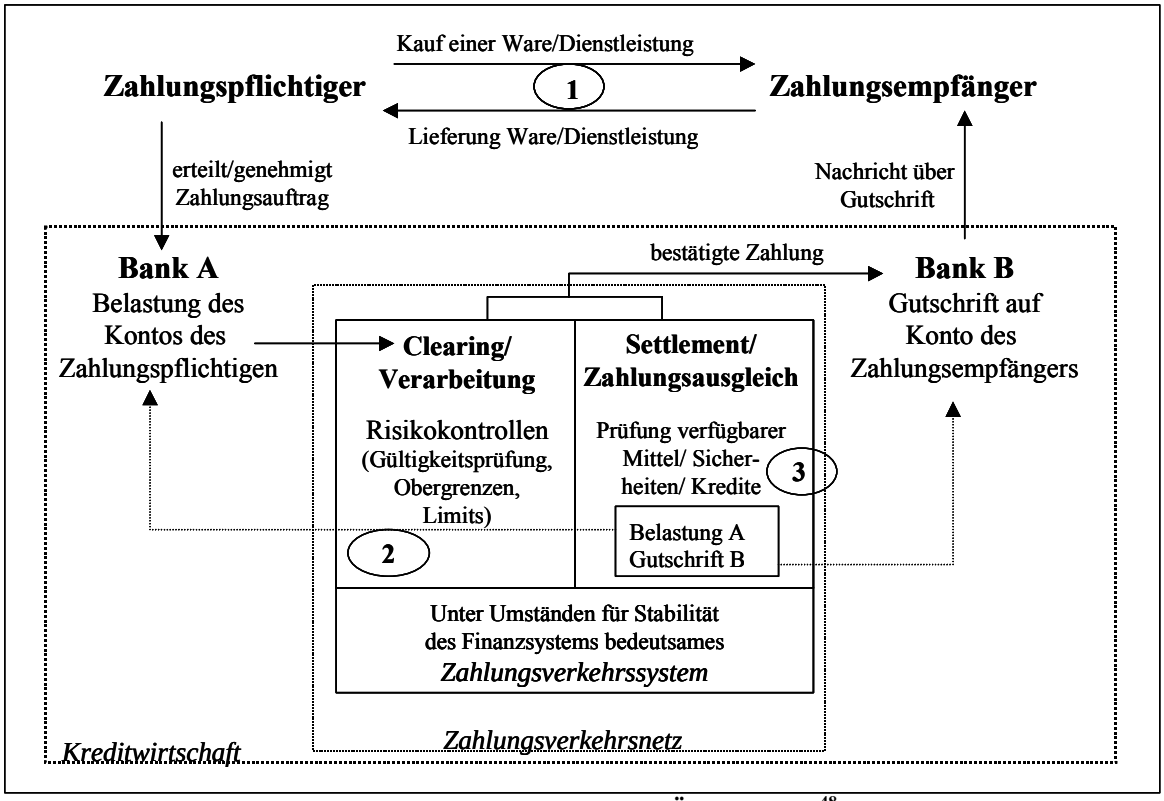

Abbildung 5: Ablauf einer Zahlungstransaktion am Beispiel Überweisung[48]

2.5 Regulierung: Begriffsbestimmung und erweiterte Arbeitsdefinition

Es gibt keine einheitliche Definition für den Begriff der Regulierung. Beispielsweise kann unter Regulierung das Erheben von Steuern und Abgaben durch den Staat verstanden werden oder in noch weiterem Sinne sämtliche Formen sozialer Kontrolle oder Einflusses, die vom Staat ausgehen.[49]

In erster pragmatischer Näherung kann Regulierung verstanden werden als „sustained and focused control exercised by a public agency over activities that are valued by a community“[50]. Allerdings sind an dieser Stelle bereits Wertungen enthalten. Es wird von einem anhaltenden Erfolg (sustained) der Maßnahme ausgegangen und zielführendes (focused) Verhalten angenommen. Wie schwer es ist, angemessen zu regulieren, zeigt sich bei der gegenläufigen Bewegung in freien Marktwirtschaften: Deregulierung verschiedener Märkte –

[48] In Anlehnung an BIZ (2001b deutsch), S. 26.
[49] Vgl. Baldwin (1999), S. 2.
[50] P. Selznick (1985): Focusing Organisational Research on Regulation“ in Noll, R. (Hrsg.) (1985): Regulatory Policy and the Social Sciences, Berkeley, zitiert in Baldwin (1999), S. 2, FN 3.

Strommarkt, Telekommunikationsmarkt, Wasserversorgung – steht auf der politischen Agenda seit einigen Jahren weit oben.

Eine im deutschen Sprachraum gängige Definition staatlicher Regulierung vermeidet jede Wertung: „Staatliche Regulierung umfasst alle hoheitlichen Eingriffe in die Gewerbe- und Vertragsfreiheit, die nicht allein der Festlegung und Durchsetzung allgemein gültiger Spielregeln der Marktwirtschaft dienen“[51].

Gewöhnlich wird unter Regulierung der Eingriff staatlicher Stellen in die Privatwirtschaft und den Wettbewerb verstanden. In der vorliegenden Arbeit wird der Begriff der Regulierung erweitert, und sowohl auf diese Form staatlicher Einflussnahme als auch auf privatwirtschaftliche Regulierung und Mischformen der Regulierung, bei der staatliche und privatwirtschaftliche Stellen zusammenarbeiten, angewendet. Privatwirtschaftliche Regulierung ist im Rahmen dieser Arbeit durch das kooperative Zusammenwirken privater Akteure und Wettbewerber im Zahlungsverkehr gekennzeichnet.

Für den Finanzsektor erscheint diese Ausweitung des Regulierungsbegriffs gerechtfertigt und notwendig, da in diesem aus verschiedenen Gründen wettbewerblich teilgeschützten Bereich erweiterte Formen der Regulierung eine besondere Rolle spielen. Beispielhaft sei auf die notwendigen privatwirtschaftlichen Anstrengungen der Kreditkartenorganisationen verwiesen über vertragliche Regelwerke und damit Regulierung im weiteren Sinne ein weltweites Netz an Akzeptanzstellen aufzubauen, welches den Besitz einer Kreditkarte für Konsumenten erst attraktiv macht.

Mischformen der Regulierung sind im Sinne der vorliegenden Arbeitsdefinition die Bereiche, in denen Markt und staatliche Regulierer in Gremien, Arbeitskreisen und Normierungsinstitutionen kooperieren und gemeinsam Regularien entwickeln. Der Zahlungsverkehr in Deutschland beispielsweies fußt maßgeblich auf den Zahlungsverkehrsabkommen, die zwischen dem Zentralen Kreditausschuss (ZKA) – und damit faktisch der gesamten Kreditwirtschaft – und der Bundesbank vereinbart wurden, und auch noch weiterhin werden.

Auf europäischer Ebene lassen sich solche Strukturen ebenfalls in ersten Ansätzen erkennen. Die Europäische Kommission verwendet dabei die Begriffe der „Ko-Regulierung“ und der „Selbstregulierung“. Unter Ko-Regulierung wird demzufolge verstanden, „dass ein Rechtsakt der Gemeinschaft die Erreichung der vom Gesetzgeber festgelegten Ziele einschlägig anerkannten Akteuren (Wirtschaftsteilnehmer, Sozialpartner, regierungsunabhängige Organisationen oder europäische Vereinigungen und Verbände) überträgt.“[52] Ko-Regulierung gibt es im Zahlungsverkehr bislang in Deutschland und auf europäischer Ebene nicht. TÜV und Dekra sind im Bereich der Überprüfung technischer Sicherheit von Produkten ein Beispiel für Ko-Regulierung. Unter Selbstregulierung versteht die EU-Kommission „die Möglichkeit für Wirtschaftsteilnehmer, Sozialpartner, regierungsunabhängige Organisationen oder Vereinigungen und Verbände, untereinander und für einander gemeinsame Leitlinien auf europäischer Ebene festzulegen (Verhaltenskodizes, sektorbezogene Vereinbarungen u.a.)“.

2.6 Zahlungsverkehr und Sicherheit: Problemorientierte Einführung

Kritische Infrastrukturen sind mit den Ereignissen am 11.9.2001 in den Mittelpunkt vielfältiger und weitreichender Untersuchungen gerückt. Allerdings gab es auch vorher bereits einschlägige Arbeitsgruppen, die sich mit der Thematik kritischer Infrastrukturen auseinander

[51] Müller (1979), S. 343.
[52] KOM (2003b), S. 18, FN 25.

setzten. Beispielsweise die interministerielle Arbeitsgruppe Kritische Infrastrukturen (KRITIS), die von der Bundesregierung Anfang 1998 auf Initiative des Bundesministers des Innern gegründet wurde. In einem ersten „Sensibilisierungsbericht KRITIS“ sollten für ausgewählte „Infrastrukturen Gefährdungen, Angriffswege, gegebenenfalls Detektionsmaßnahmen und Lösungsvorschläge“[53] aufgezeigt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI), zuständig für die Fortführung der KRITIS-Arbeiten, hat für weitere Untersuchungen die Infrastruktur in Deutschland in Übereinstimmung mit internationalen Ansätzen in sieben kritische Substrukturen unterteilt: die Bereiche Telekommunikation, Energieversorgung, Transport- und Verkehrswesen, Gesundheitswesen, Notfall- und Rettungsdienste, Regierung und öffentliche Verwaltung und das Bank-, Finanz- und Versicherungswesen.

Zahlungsverkehr als Teil des Finanzwesens ist als volkswirtschaftliche Querschnittfunktion verschiedenen Gefahren ausgesetzt. Zunächst gilt es, die kritische Infrastruktur, auf der Zahlungsverkehrstransaktionen ausgeführt werden, zu schützen, damit nicht das gesamte System und darüber hinaus die Volkswirtschaft gefährdet wird. Allerdings sind Angriffe existentieller Art auf kritische Infrastrukturen – nicht nur den Zahlungsverkehr – in den Industrieländern seit dem 2. Weltkrieg in erster Linie auf Planspielniveau angesiedelt; bis auf den 11. September gibt es keine empirische Evidenz. Dies bedeutet nicht, dass das Risiko zu unterschätzen wäre: Untersuchungen gehen von einer hohen systemischen Verwundbarkeit kritischer Infrastrukturen aus, bei gleichzeitig relativ geringem Mitteleinsatz – wenngleich ein hohes Maß an für die Durchführung von Angriffen notwendigem technischen Know-How unabdingbar erscheint.[54] Ein Musterbeispiel liefert der Fall einer in den USA verfassten Doktorarbeit eines Geographen, dem es mit öffentlich zugänglichen Quellen gelungen ist, ein Programm zu schreiben, das die Glasfaser-Netzwerke nicht nur in ihrer Lokalisierung beschreibt, sondern auch noch die darüber laufenden Informationen nach Branchen trennen kann.[55] Mit der Software lässt sich ferner bestimmen, an welchen Stellen simple Störungen des Glasfaser-Netzwerks maximalen Schaden anrichten könnten. Bemerkenswert, dass die Arbeit in den USA erst durch die Ereignisse des 11.09.2001 ins Rampenlicht der Öffentlichkeit geraten ist; vorher hatten selbst Fachleute kein ausgeprägtes Interesse an diesem Thema.

Anders sieht es mit den Risiken aus, die Schaden in unterschiedlicher Höhe aber nicht zwangsläufig von systemischen Ausmaßen auslösen können. Dazu zählen unter anderem Probleme im Bereich Kreditkartenbetrug und weitere Schadensfälle, bei denen organisatorische Schwächen im System ausgenutzt werden, um hohe Millionenbeträge betrügerisch zu transferieren.

Auf dem Gebiet elektronischer Zahlungssysteme besteht ein grundsätzliches Problem der Datenerhebung unter dem Aspekt quantifizierbarer Sicherheit.[56] Banken sind von der Natur ihres Kerngeschäfts Institutionen, die von dem Vertrauen leben, das ihnen entgegengebracht wird. Die Publizität von Schadensereignissen jeglicher Art, in besonderem Maße von Schadensereignissen, die im Erfahrungshorizont der Öffentlichkeit liegen, ist gegen die Geschäftsinteressen der Kreditwirtschaft gerichtet. Demzufolge werden Schadensfälle soweit wie möglich intern bearbeitet und nicht nach außen kommuniziert. Die Brisanz des Themas

[53] KRITIS (1999), S. 4.
[54] Vgl. Münch (2002), KRITIS (1999).
[55] Vgl. Traufetter (2003).
[56] Eine Schwierigkeit, die insgesamt bei der Erhebung Operationeller Risiken auch bei der sogenannten Quantitative Impact Study der Bank für Internationalen Zahlungsausgleich im Rahmen der Kalibrierung von Basel II eine große Rolle spielt(e). Die zeitliche Verzögerung bei der Implementierung von Basel II geht nicht zuletzt auf Probleme der Datenerhebung zurück, die eine Berechnung der Auswirkungen der neuen Regelungen erschwerte.

wird gleichwohl bereits anhand der öffentlich gewordenen Schadensfälle überdeutlich (vgl. ausführlich Abschnitt 5.3.2.1).

Ein Beispiel verdeutlicht die Risiken im Internet: Die Nutzung der Kreditkarten im Internet ist unkompliziert, der Betrug bislang auch. Die Banken und Kreditkartengesellschaften versuchten dem Problem durch die Einführung des SET-Standard, der Anfang 2002 in VISA 3D (Three Domain, nunmehr „Verified by VISA") und UCAF/SPA (Universal Cardholder Authentification Field/Secure Payment Application, nunmehr MasterCard SecureCode) übergegangen ist, zu entgehen.[57] Laut Urteil des Bundesgerichtshofs ist aber bereits gemäß § 9 I AGBG (Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen) eine Missbrauchsklausel unwirksam, die das Missbrauchsrisiko allein auf den Karteninhaber überwälzt. Die Kreditinstitute tragen die Beweislast.[58]

Wie schnell auf der rechtlich-ökonomischen Ebene etablierte Geschäftsprozesse im Zahlungsverkehr beeinflusst werden können, zeigt für den Kreditkartenmarkt eine Gerichtsentscheidung des Bundesgerichtshofs (BGH) von 2002.[59] Es wurde die bisherige Praxis, Akzeptanzverträge als Forderungskauf zu sehen, in Frage gestellt. Sie sind in Zukunft als abstraktes Schuldversprechen zu bewerten, und die Verträge daraufhin umzuformulieren. Dies hat zur weitreichenden Konsequenz, dass die Haftung den Kreditkartenunternehmen respektive dem Acquirer[60] zum großen Teil mit auferlegt wurde. In der Folge wurde die schnellstmögliche Kündigung der Kreditkartenakzeptanzverträge durch die Kreditkartenunternehmen betrieben, um die neuen Konditionen in neuen Verträgen wirksam werden zu lassen. Dies brachte zunächst den Markt für neue Verträge insbesondere für kleinere Händler ohne erwiesene Bonität und bestehenden großen Kundenstamm zum Erliegen.[61] Ferner hatte diese Entscheidung die gängige Praxis für rechtswidrig erklärt, nach der Kreditkartenakzeptanzverträge für Händler im Mail-Order/Telephone-Order Bereich eine Klausel enthielten, mit der die Haftung im Missbrauchs- und Betrugsfall einseitig auf die Seite der Vertragsunternehmen verlagert wurde. Der BGH sah in dieser Vereinbarung eine unangemessene Benachteiligung der Händler, da diese kaum einen Einfluss auf die Bekämpfung des Kreditkartenmissbrauchs hätten. Die Tatsache, dass ein höchstes deutsches Gericht sich mit diesem Thema auseinandersetzt, und dabei ein 12 Jahre altes Urteil revidiert, zeigt die Bedeutung, die Schadensfälle durch betrügerische Maßnahmen bei Kreditkartenzahlungen mittlerweile erreicht haben. Offensichtlich gehen der Justiz die angekündigten Verbesserungen auf der Sicherheitsebene der Kreditkartenorganisationen („Verified by Visa" und MasterCard „SecureCode") nicht weit genug, mit der solche Probleme in absehbarer Zeit gelöst werden könnten.

Operationelle Risiken berühren ferner unter anderem die Haftungsbeschränkungen der Bank in ihren Allgemeinen Geschäftsbedingungen. Die Bank darf laut Urteil des Bundesgerichtshofs (BGH) ihre Haftung für technisch oder betrieblich bedingte zeitweilige Beschränkungen und Unterbrechungen ihres Servers nicht umfassend ausschließen.[62]

---

[57] Vgl. zu den Verfahren im Detail: 4.2.6.4.1.
[58] Brisch, R., in: Secunet (2001), S. 16.
[59] Bundesgerichtshof: Urteil Az. XI ZR 375/00. Der BGH gibt damit die Position auf, die im Urteil vom 2.5.1990 Az. VIII ZR 139/89, WM 1990, 1059, festgelegt wurde und Akzeptanzverträge für Kreditkarten mit Forderungskauf gleichgestellt hatte. Ferner wird die Unwirksamkeit einer Klausel in den AGB von Kreditkartenunternehmen, die auch bei schuldlosem Scheitern einer Zahlung die Haftung auf den Händler abwälzt, unter Bezug auf § 9 II Nr. 2 AGBG höchstrichterlich festgestellt. Vgl. NWIR (2002).
[60] Acquirer: Die Bank, die Händlern Kreditkartenverträge vermittelt.
[61] Vgl. Bartsch (2003).
[62] Vgl. Brisch, R., in: Secunet (2001), S. 15.

Die Bedeutung organisatorischer Bestimmungen innerhalb der Institute zur Verhinderung von Schadensfällen durch Operationelle Risken im Zahlungsverkehr wird durch einzelne Betrugsfälle und -versuche vor Augen geführt. Ein Musterbeispiel ist der verhinderte Transfer von über USD 30 Mio. ins Ausland, durchgeführt von einem Innentäter, der alle technischen Hürden genommen hatte und an einem Kontrollanruf scheiterte, der ab einer Höhe von USD 20 Mio. zwischen den teilnehmenden Banken nötig war, und von dem der Täter nichts gewusst hatte.[63]

Spätestens seit der Diskussion um Operationelle Risiken in Basel II und der Pflicht, diese Risiken zukünftig mit Eigenkapital zu unterlegen, rückt auch der Bereich des Risikomanagements elektronischer Zahlungssysteme in (offenen) Netzen verstärkt ins Blickfeld aufsichtlicher Regelungen und bankinterner Maßnahmen. Mit der Frage, wie Sicherheit in elektronischen Zahlungssystemen in Zukunft effektiv erreicht werden kann, und welche Rolle dabei die regulatorischen Bemühungen hoheitlicher und privatwirtschaftlicher Stellen spielen sollen, können oder müssen, beschäftigt sich diese Arbeit im Folgenden.

[63] Vgl. Thodén (2000), S. 67.

3 Regulierung: Allgemeine Grundlagen und bankspezifische Besonderheiten

3.1 Grundlagen der Regulierung

3.1.1 Motivation staatlicher Regulierung der Wirtschaft

Regulierung lässt sich in der Theorie aus verschiedenen Blickwinkeln betrachten. Baldwin und Cave identifizieren bei ihrer umfassenden Systematisierung mindestens fünf Grundtypen oder „Schulen" der Regulierungstheorie.[64] Versucht wird bei allen, das Zustandekommen von Regulierung theoretisch zu untermauern oder machttheoretisch zu begründen, um die Thesen anschließend empirisch zu überprüfen. Die neueren institutionenökonomischen Ansätze erweitern die Diskussion um das Für und Wider von Regulierung, und verdeutlichen die Schwäche normativer Ansätze, allerdings um den Preis zunehmender Komplexität und Angreifbarkeit der Argumentation.

Die Gründe, mit denen Eingriffe in die Marktfreiheit gerechtfertigt werden, sind je nach staatlichem Selbstverständnis und vorherrschender politischer Lage unterschiedlich. In der Regel ist erwartetes oder bereits eingetretenes Marktversagen die Motivation für Regulierung. Jede Form staatlicher Eingriffe in den Markt bewegt sich in dem Spannungsfeld zwischen dem Wunsch, durch Regulierung Einfluss in einer sozial erwünschten Form auf den Markt zu nehmen, und der Stagnation des Marktes aufgrund eben dieser Regulierung – oder der zu flexiblen Reaktion des Marktes, der versucht, Regulierungen zu unterlaufen.

Verschiedene Begründungen und damit zugleich Ziele hoheitlicher Regulierungsbemühungen in Märkten – abseits eventuell auftretender Interessenkonflikte und einseitiger Einflussnahme – lassen sich nach Baldwin unterscheiden.[65] Dazu zählen unter anderem:

- Marktversagen kann zu Monopolbildung und Monopolpreisen führen, die gesamtwirtschaftlich unerwünscht sind. Gleiches gilt für natürliche Monopole, die entstehen, aber wünschenswert sein können, falls auftretende Skaleneffekte die ausreichende Produktion eines Gutes durch nur eine Firma ermöglichen.
- Externe Effekte (Externalitäten oder Spillovers) stellen eine wesentliche Motivation für regulierende Maßnahmen dar. Treten externe Effekte auf, wird ein Teil der gesamtwirtschaftlichen Kosten eines Produkts nicht über den Marktpreis reflektiert und kann so zu unerwünschtem Verhalten der Marktteilnehmer führen.
- Informationsasymmetrie ist ein weiterer Grund für Regulierungsbemühungen. Im theoretisch vollkommenen Markt wird von einer Symmetrie der Informationsverteilung ausgegangen. Auf dieser Grundlage können marktwirtschaftliche Entscheidungen getroffen werden. Wird diese Symmetrie aus verschiedensten Gründen gestört, kann der Markt nicht ordnungsgemäß funktionieren, Regulierung erscheint in bestimmten Fällen notwendig. Dabei darf nicht übersehen werden, dass ebendiese Informationsasymmetrie und die unterschiedliche Einschätzung der Informationen als Triebkraft der Märkte gesehen werden.
- Die gesamtgesellschaftlich gewünschte Verfügbarkeit und Reichweite bestimmter Dienstleistungen kann vom Markt nicht gewährleistet werden. Mit Hilfe der Regulierung können Marktteilnehmer zur flächendeckenden Erfüllung bestimmter Aufgaben motiviert werden.

[64] Vgl. Baldwin (1999), S. 19 ff. und die dort angegebene zahlreichen Literaturhinweise, die meist im Feld der politischen Ökonomie angesiedelt sind.
[65] Vgl. Baldwin (1999), S. 7ff.

- Funktionierender Wettbewerb wird möglicherweise nur durch Regulierung, beispielsweise in Form von Kartellbehörden, möglich. Ansonsten droht wettbewerbswidriges Verhalten, seien es unzulässige Kartellabsprachen oder verschiedene Ausprägungen ruinösen Wettbewerbs[66], beispielsweise Dumpingpreise, um Wettbewerber aus dem Markt zu drängen. Eine besonders schädliche Form ruinösen Wettbewerbs entsteht bei unelastischer Nachfrage, die zu volkswirtschaftlich ungünstiger Ressourcenverwendung im großen Stil führen kann.
- Öffentliche Güter, z. B. Bildung/Kultur, Medieninhalte, Verkehrsinfrastruktur, können vielfach nur über (teil-)regulierte Regime am Markt untergebracht werden. Sonst drohen aufgrund von Free Rider Problemen und auftretendem Moral Hazard volkswirtschaftlich unerwünschte Effekte.
- Regulierung kann begründet werden, falls der Sozialstaat als „wohlmeinender Diktator" gesehen wird, der Partikularinteressen aus vermeintlichem oder tatsächlichem Wissen heraus begrenzen sollte. Ein Beispiel ist das Verbot von öffentlicher Tabakwerbung aus gesundheitspolitischen Motiven.
- Sollen bestimmte übergeordnete Ziele, beispielsweise intergenerationelle Gerechtigkeit oder nachhaltiges Wirtschaften erreicht werden, kann sich der Markt als inadäquates Instrumentarium erweisen, da der Zeithorizont möglicherweise zu kurz ist. In diesem Fall sollen regulierende Maßnahmen ein solches Defizit beheben.

3.1.2 Regulierungsinstrumente

Regulierungsinstrumente lassen sich grundsätzlich in zwei Kategorien einteilen: Fiskalische und marktorganisatorische Maßnahmen.[67]

Bei fiskalischen Instrumenten können direkte und indirekte fiskalische Eingriffe unterschieden werden. Bei den direkten Maßnahmen greift der Staat unmittelbar nicht nur regulierend, sondern aktiv gestaltend in den Markt ein und bietet in Eigenregie, das heißt durch die Gründung von Staatsunternehmen oder durch die Verstaatlichung bestehender Unternehmen, Produkte und Dienstleistungen auf dem Markt an. Im Bankensektor ist der gesamte Bereich der öffentlich-rechtlichen Kreditwirtschaft unter staatlicher Einflussnahme und insbesondere mit der Gewährträgerhaftung der öffentlichen Hand geschützt; es ist vor dem Hintergrund europäischen Rechts und den Bemühungen der Geschäftsbanken gegen diese aus ihrer Sicht vorhandene Wettbewerbsverzerrung jedoch fraglich, ob dieser Einfluss von Dauer sein wird. Bei den indirekten Eingriffen geht die hoheitliche Intervention einen anderen Weg; über sektorspezifische Steuern, Abgaben oder Subventionen wird versucht, einen Lenkungseffekt zu erzielen.

Zu den marktorganisatorischen Instrumenten zählen ordnungspolitische und prozesspolitische Handlungen. Mit dem ordnungspolitischen Instrumentarium wird auf die Wirtschaft verhaltensregulierend eingewirkt, beispielsweise mit Normvorgaben für bestimmte Vertragsgestaltungen oder mit Mindeststandards; der Rahmen für das Wirtschaften eines Sektors wird vorgegeben. Eine direkte Regulierung einzelner Marktteilnehmer findet mit prozesspolitischen Maßnahmen statt, bei denen der Marktmechanismus außer Kraft gesetzt wird, unter anderem durch Marktzutrittsbarrieren (z. B. Banklizenz nach Kreditwesengesetz), Investitionskontrollen, Mengenkontingentierung oder Preiskontrollen (z. B. EU-Verordnung 2560/2001/EG zum grenzüberschreitenden Zahlungsverkehr). Auch mit Ausschreibungen (Wettbewerbslösung), die bestimmte Standards setzen oder fordern, kann regulierend in den Markt eingegriffen werden.

[66] Vgl. Kupitz (1983), S. 124 ff.
[67] Vgl. Morasch (2002), S. 90f.

3.2 Regulierung des Finanzsektors

Der Finanzsektor mit seinen Märkten für Bank- und Finanzdienstleistungen gehört international zu den am stärksten regulierten Wirtschaftszweigen.[68] Gleichwohl stellen Dewatripont und Tirole ernüchtert fest: „There is no consensus in academe on why banks should be regulated, how they should be regulated, and whether they should be regulated at all."[69] Welche Argumentation und rechtlichen Grundlagen für die aktuelle Regulierung des Finanzsektors gelten, wird in den folgenden Abschnitten dargelegt.

Historisch gesehen wurde das Geflecht regulatorischer Bemühungen um die Stabilität des Finanzsektors erst im 20. Jahrhundert entwickelt.[70] Während noch in der letzten Hälfte des 19. Jahrhunderts die Versuche scheiterten, eine allgemeine Bankenaufsicht im Rahmen der Diskussion um ein Bankgesetz im Gefolge der Gewerbeordnung einzuführen, wurde der Druck mit dem Konkurs von Privatbanken um die Jahrhundertwende höher. Allerdings führte erst die Bankenkrise im Rahmen der Weltwirtschaftskrise im Jahre 1931 zur Einführung einer allgemeinen Bankenaufsicht. 1934 wurde das Kreditwesengesetz (KWG) verabschiedet. Die Bankenaufsicht wurde nach dem 2. Weltkrieg dem Finanzministerium unterstellt, das KWG blieb gültig und wurde seitdem in mehreren Novellen aktualisiert. Die 6. Novelle wurde 1997 verabschiedet, mit dem 4. Finanzmarktförderungsgesetz, einem Artikelgesetz, das verschiedene Gesetze modifiziert, wurde Mitte 2002 das KWG an die E-Geld-Richtlinie der EU angepasst.

Institutionell ist die Bankenaufsicht nach dem 2. Weltkrieg von politischen Machtfragen geprägt. Die zentrale Aufsicht durch das Bundesaufsichtsamt für Kreditwesen (BAKred) wurde zunächst zugunsten dezentraler Aufsichtsorgane auf Länderebene verhindert und erst mit der 1. Novelle des KWG 1962 realisiert.

Die Entwicklung des bankaufsichtlichen Rechts lässt sich anhand akuter Problemlagen, beispielsweise folgt die 2. Novelle des KWG der Herstatt-Krise im Jahr 1974, verfolgen. Es gab nach 1962 keine grundlegende Neukonzeptionierung der Bankenaufsicht und ihren Rechtsgrundlagen. Wesentliche Impulse für Veränderungen kommen insbesondere von der Harmonisierung des Bankenrechts auf europäischer Ebene, so wurden die 4., 5. und 6. Novelle des KWG durch die EG-Bankrechtsharmonisierung, unter anderem die EG-Bankrechtskoordinierungsrichtlinie, die Großkreditrichtlinie, die Konsolierungsrichtlinie und die EG-Kapitaladäquanzrichtlinie, begründet. Die 6. Novelle des KWG etablierte neben den Finanzinstituten eine weitere institutionelle Form, die Finanzdienstleistungsinstitute, die ebenfalls der Aufsicht unterliegen. Neuen technologischen Möglichkeiten wurde Tribut gezollt, und unter anderem das Geldkartengeschäft und das Netzgeldgeschäft als Bankgeschäft definiert, und somit der Aufsicht unterworfen – ein Vorgehen, das zeigt wie flexibel die Aufsichtsbehörden potenzielle kritische Entwicklungen für die systemische Sicherheit per Gesetzgebung auffangen können.[71]

[68] Vgl. Bonn (1998), S. 36 und Büschgen (1998), S. 253.
[69] Vgl. Dewatripont (1994), S. 29. Zum gleichen Schluss kommt Santos (2000), S. 5.
[70] Die Ausführungen über die historischen Entwicklungslinien beruhen auf Büschgen (1998), S. 253 ff.
[71] Vgl. ausführlich Hartmann (2000).

3.2.1 Motive für eine besondere Regulierung des Finanzsektors

Zwei Argumentationsmuster lassen eine Regulierung des Bankensektors aus staatlicher Sicht angemessen und notwendig erscheinen:[72]

1) Marktversagen: Wird die Funktionsfähigkeit von Märkten kritisch beurteilt, wird Regulierung erforderlich. Über die Wohlfahrtseffekte einer solchermaßen verstandenen Regulierung lässt sich trefflich streiten.
2) Systemische Risiken: Wird der Bankenmarkt als ein aufgrund sektorspezifischer Besonderheiten gefährdetes Subsystem verstanden, bei dem Marktversagen in Finanzmarktinstabilität enden kann, wird Regulierung ebenfalls wünschenswert. Idealerweise erfolgt diese kooperativ mit dem Markt, um den gesamtwirtschaftlichen Nutzen zu maximieren.

Das Kreditwesengesetz als wesentliche Grundlage bankenspezifischer Regulierung in Deutschland wird in seiner Konzeption übereinstimmend der zweiten Sichtweise zugeordnet.[73]

Bankgeschäfte werden im Vergleich zu sonstigen marktwirtschaftlichen Prozessen als besonders „vertrauensempfindlich" eingestuft. Marktversagen kann in diesem Fall volkswirtschaftlich besonders schädlich wirken. Zwei zentrale Argumente für die Notwendigkeit einer Regulierung finden sich in jeder Abhandlung zu diesem Thema: a) das Risiko einer systemischen Krise und b) das Einlegerschutzargument.[74] Das Einlegerschutzargument kann direkt mit der „Vertrauensempfindlichkeit" von Bankgeschäften begründet werden; damit sich Bankgeschäfte überhaupt gesamtgesellschaftlich wohlfahrtsteigernd durchsetzen können, muss der Staat mit seiner Regulierung Vertrauen in die Einlagensicherung (eigentlich in die Bankenlandschaft generell) gewährleisten. Im Sinne einer korrekten Systematisierung stellt das Einlegerschutzargument nur eine Untergruppe der Argumente dar, die Regulierung mit der Gefahr systemischer Risiken begründen. Im Kern der systemischen Risiken steht die Sorge vor einem Sturm auf die Banken (engl. bankrun), einer Bankenpanik, bei der alle Einlagen von den Anlegern gleichzeitig abgezogen zu werden drohen.[75] Historische Erfahrungen dieser Art wurden in der Weltwirtschaftskrise der 30-iger Jahre des letzten Jahrhunderts gemacht. Volkswirtschaftlich würde ein solcher Vertrauensverlust der Bürger in die Bankenlandschaft einen maximalen Schaden anrichten können – in der Folge rechtfertigt die Kontrolle systemischer Risiken den Einsatz hoheitlicher Aufsichtsmaßnahmen.

Abgeleitet von den theoretischen Fällen eines Marktversagens, die bereits in Kapitel 3.1.1 allgemein diskutiert wurden, können weitere Argumente, die teils auf die beiden oben genannten zentralen Begründungen zurückführen, für die staatliche Regulierung (und ebenso wohlfahrtsökonomische Kritikpunkte an dieser Regulierung) der Kreditwirtschaft (nicht beschränkt auf den Zahlungsverkehrs) abgeleitet werden:[76]

Mögliches Auftreten natürlicher Monopole im Bankensektor: Die Notenbank hat in bestimmten Bereichen ein staatlich gewünschtes (natürliches) Monopol, das für den Bereich der

[72] Vgl. Burghof (1996), S. 18.
[73] Vgl. Burghof (1996), FN 44, Fabritius (2001), S. 3 f.
[74] Gelegentlich findet sich als drittes Argument das Kostenkontrollargument (vgl. Burghof (1996), S. 20), bei dem es sich eigentlich aber um eine Ausprägung des Einlegerschutzargumentes handelt, da es bei diesem Argument nur um die Kosteneffizienz der staatlichen Aufsicht geht, die schlicht als billiger eingeschätzt wird als private Kontrolle.
[75] Vgl.ausführlich Santos (2000), S. 5 ff.
[76] Vgl. Santos (2000), S. 20 f., Dewatripont (1994), S. 29 ff. und Kupitz (1983).

Banknotenemission in § 14 Abs. 1 Bundesbankgesetz verankert ist, und mittlerweile auf das Eurosystem ausgedehnt wurde. Auch die Bankenaufsicht als hoheitliche Aufgabe lässt sich, da die Kosten der Überwachung sehr hoch und schlecht teilbar sind, über ein natürliches Monopol begründen. Bei den Geschäftsbanken wäre ein natürliches Monopol unerwünscht, allerdings haben weder empirische Studien noch theoretische Überlegungen die für ein natürliches Monopol notwendige Subadditivität der Kostenfunktionen (technisch-organisatorisch und liquiditätsmäßig-finanziell) nachweisen können.[77] Phasen der Expansion kleinerer Kreditinstitute, wie sie bis in die achtziger Jahre auftraten[78], wechseln mit Fusions- und Verdrängungsphasen, die aktuell die Bankenlandschaft dominieren, ab. Dabei scheinen eher wettbewerbliche Aspekte eine Rolle zu spielen als Tendenzen zu natürlichen Monopolen. Anders könnte die Lage aussehen, wenn die Transaktionsbanken, die zur Zeit von deutschen Großbanken gegründet werden, tatsächlich technisch-organisatorisch so große Effizienzgewinne mit sich brächten, dass Monopolisierungstendenzen erkennbar würden. Die Effizienzbemühungen zeigen sich deutlich am Beispiel der geplanten Transaktionsbanken, bei denen es den beteiligten Banken darum geht, möglichst viele automatisierbare Prozessschritte im „back-office"-Bereich in eine für den Kunden nicht sichtbare „back-office"-Bank kosteneffizient zu verlagern.[79]

Unerwünschte externe Effekte: Regulatorische Maßnahmen der Bankenaufsicht, die ganz allgemein das Risiko des Bankensektors minimieren, dienen der Vermeidung externer Effekte – da weder die einzelne Geschäftsbank noch der Privatanleger ihr Verhalten am Gemeinwohl orientieren und somit bestimmte Risikosituationen zu Bankrun-Verhalten führen könnten. In andere Richtung geht das Geldschöpfungsargument: Regulierung, in diesem Fall Wettbewerbsbeschränkung der Geschäftsbanken bei der Geldschöpfung, soll den Kaufkraftverfall verhindern, der infolge externer Effekte aus unbegrenzter Emission von Geschäftsbankengeld resultieren würde. Wird jedoch der Wettbewerb so sehr beschränkt, dass die Geschäftsbanken günstige Zinsänderungen bei expansiver Geldpolitik nicht mehr unmittelbar an den Markt weitergeben müssten, wäre die Geldpolitik unter Umständen durch Time-Lags[80] behindert.[81]

Marktversagen aufgrund von Informationsasymmetrie oder unvollständigen Informationen: In der Sicht der Institutionenökonomik birgt eine Schuldner-Gläubiger-Beziehung verschiedene Risiken, die bei Bankgeschäften dementsprechend wirksam werden können. Der Agent (Schuldner/Unternehmen, das einen Kredit nimmt) besitzt bessere Informationen über seine eigentliche Situation als der Prinzipal (Gläubiger, Bank), insbesondere bei mehrperiodigen Investitions- und Finanzierungsentscheidungen kann der Agent entgegen den Interessen des Prinzipals handeln (hidden action), ohne das dieser Einfluss nehmen kann (Moral Hazard), es sei denn um den Preis hoher Kontrollkosten, die den Vertrag eventuell ex ante unrentabel für den Schuldner machen würden. Die Verteilung des Risikos – der Schuldner steigert in Erwartung höherer Gewinne seine Risikobereitschaft – und der Risikoprämie – im Erfolgsfall profitiert nur der Schuldner, der Gläubiger bekommt einen festen Zinssatz – ist zuungunsten des Gläubigers verteilt.[82] Hier scheint das Einlegerschutzargument durch. Der Einleger kann die Kreditvergabe und die Risikoposition der Bank und das Verhalten des Bankmanagements nicht beurteilen und ist, angesichts der ohnehin niedrigen Eigenkapitalquote von Banken, auf

[77] Tichy (1990), S. 382: „Es gibt wenig Evidenz für merklich steigende Skalenerträge, außer bei sehr kleinen Banken; die Verbundvorteile einer Ausweitung der Produktpalette dürften sich in engen Grenzen halten.", zitiert in Burghof, S. 31, FN 31.
[78] Vgl. Kupitz (1983), S. 80 ff.
[79] Vgl. Ketterer (2003).
[80] Der Begriff Time-Lag wird hier verstanden als Wirkungsverzögerungen der Transmissionsmechanismen bei der Geldpolitik, Vgl. Duwendag et al. (1999), S. 169 f.
[81] Vgl. Seifert (1984), S. 154 ff.
[82] Vgl. Bonn (1998), S. 36ff.

eine staatliche Aufsicht angewiesen; andernfalls droht Vertrauensverlust der Einleger. Asymmetrische Informationen können auch zum Problem adverser Selektion führen. In diesem Fall kann der Bankkunde die Qualität von Bankprodukten nicht abschätzen und neigt dazu, vermeintlich hochpreisige Produkte zu vermeiden und Produkte durchschnittlicher Marktqualität zu wählen. In der Folge verschwinden qualitativ hochwertige Anbieter vom Markt, die Durchschnittsqualität sinkt.[83] Beispielsweise könnten Lebensversicherer, denen es nicht gelingt, ihr im Vergleich zum Markt risikobewussteres Anlageverhalten den Marktteilnehmern zu kommunizieren, in bestimmten Marktphasen (hohe Rendite bei risikobehafteter Anlage, ohne entsprechende Ausfälle in Boomzeiten) aus dem Markt gedrängt werden, da die Konditionen für die Marktteilnehmer unattraktiv wirken. Eine ähnliche Problematik wäre bei Zahlungssystemanbietern, die Einlagen der Teilnehmer verwalten, denkbar. Ein Effekt, der aus Sicht der Aufsicht unerwünscht ist.

Inwieweit diese Argumente tatsächlich eine regulatorische Ausnahmestellung der Kreditwirtschaft rechtfertigen, bleibt umstritten. Beispielsweise gehen Kunden auch mit anderen Unternehmen langfristige Geschäftsbeziehungen ein, ohne dass diese oder jene Branche verstärkt reguliert würde. Die Funktionsfähigkeit dieser Märkte deutet auf eine effiziente Marktkontrolle hin und lässt im Umkehrschluss die Frage zu, warum auf dem Bankensektor nicht ähnliche Kontrollen etabliert werden konnten. Die oben skizzierten Schwierigkeiten mit Moral Hazard und adverser Selektion sind für den Finanzsektor jedoch typisch und rechtfertigen aus Geschäfts – wie aus Zentralbanksicht aufsichtliche Maßnahmen zum Schutz der kleinen Bankgläubiger.[84]

Lediglich die Bankrun-Problematik ist unumstritten, nicht zuletzt aus historischer Erfahrung, und stellt das Kernargument für die umfassende Regulierung des Finanzsektors dar. Die Erfahrungen der Weltwirtschaftskrise in Jahren 1929 bis 1933 sind weltweit Ausgangspunkt für massive regulatorische Initiativen im Bankensektor gewesen, die größtenteils bis heute Bestand haben.[85]

3.2.2 Kreditwirtschaft als wettbewerblicher Ausnahmebereich

Die postulierte Schutzbedürftigkeit der Einleger, die ihr Geld den Banken anvertrauen, hat auf der regulatorischen Ebene zu einigen Besonderheiten geführt, die unter anderem auf die Marktstruktur einen entscheidenden Einfluss hatten.

Allerdings gilt es nicht nur, die Einlage der Bankkunden vor systemischen Risiken zu schützen, auch der Wert des Geldes, Binnenwert und Außenwert, das in einer Volkswirtschaft eingesetzt wird, gilt als schutzbedürftig – und erfordert regulative Schritte. In der Folge ergibt sich basierend auf den entsprechenden Notenbankgesetzen eine Bankenstruktur, die zwischen der Notenbank, versehen mit dem Banknotenmonopol[86], und den Geschäftsbanken einerseits eine klare Trennlinie zieht, andererseits Kooperation erfordert, um die geldpolitischen Ziele der Zentralbank gemeinsam mit den Geschäftsbanken, die am Markt operieren, zu erreichen.

[83] Vgl. Burghof (1996), S. 32. Grundlage dieser Überlegungen sind die Arbeiten von Akerlof (1970), der mit dem Markt für Zitronen (Gebrauchtwagen minderer Qualität) der sich erst durch den asymmetrischen Informationsstand der Käufer und Verkäufer entwickelt, ein Musterbeispiel adverser Selektion beschreibt.
[84] Vgl. Dewatripont (1994), S. 31 f.
[85] Weitere Ausführungen und Literaturhinweise zu diesem Themenkomplex finden sich u.a. bei Burghof (1996), S. 17, FN 42 und S. 22, FN 57.
[86] § 14 Abs. 1 und 2 BBankG.

In Deutschland begründet das Gesetz gegen Wettbewerbsbeschränkungen (GWB) die Kreditwirtschaft als wettbewerblichen Ausnahmebereich.[87] Die Zielsetzung des GWB, das am 1.1.1958 in Kraft getreten ist, wird am deutlichsten aus der Begründung zum damaligen Regierungsentwurf: „...stellt eine der wichtigsten Grundlagen zur Förderung und Erhaltung der Marktwirtschaft dar. Es soll die Freiheit des Wettbewerbs sicherstellen und wirtschaftliche Macht da beseitigen, wo sie die Wirksamkeit des Wettbewerbs und die ihm innewohnende Tendenz zur Leistungssteigerung beeinträchtigt und die bestmögliche Versorgung der Verbraucher in Frage stellt."[88] In diesem Grundverständnis wird der Anwendungsbereich des Gesetzes durch die §§ 28-31, die sogenannte Ausnahmebereiche festlegen, eingeschränkt. Durch § 29 GWB wird die Kredit- und Versicherungswirtschaft partiell von den Bestimmungen des GWB entbunden. Im Einzelnen sind dies Ausnahmen bezüglich bestimmter Kartelle, Bindungen und Empfehlungen, unter anderem sind bestimmte Vereinbarungen und Preisabsprachen möglich (§14 und §22 Abs. 1 Satz 1), die anderen Branchen verboten sind.

§ 130 GWB schließt die Deutsche Bundesbank und die Kreditanstalt für Wiederaufbau völlig von den wesentlichen Regelungen des GWB aus („totaler Ausnahmebereich").[89] Die Ausnahmebereiche bedeuten jedoch keineswegs weniger Regulierung, sondern führen in direkter Linie zu weiteren Gesetzen, die im Fall der Kreditwirtschaft das Kreditwesengesetz (KWG) und das Bundesbankgesetz (BBankG) darstellen. In § 29 Abs. 5 GWB wird dies klar zum Ausdruck gebracht: „Die Absätze 1 bis 4 gelten nur für Vereinbarungen, Beschlüsse und Empfehlungen, die im Zusammenhang mit Tatbeständen stehen, die der Genehmigung oder Überwachung durch das Bundesaufsichtsamt für das Kreditwesen, das Bundesaufsichtsamt für das Versicherungswesen oder die Versicherungsaufsichtsbehörden der Länder unterliegen."[90] Erst in der Folge eines solchermaßen definierten Ausnahmebereichs ist eine Institution wie der Zentrale Kreditausschuss (ZKA) aus der Sicht des Wettbewerbsrechts zulässig. Gleichwohl spricht Riehm von einem Bankenprivileg, das für den Bereich Zahlungsverkehr den Wettbewerb ausschließt oder stark beeinträchtigt.[91]

Das KWG ist für die Institute und Unternehmen, die in seinen Geltungsbereich fallen, dazu zählen insbesondere Kreditinstitute und Finanzdienstleistungsinstitute[92], die rechtliche Grundlage der Regulierungsmaßnahmen. In § 1 Abs. 1 werden die vom KWG am stärksten regulierten Kreditinstitute über die Art der ausgeübten Geschäftstätigkeit definiert. Für den Zahlungsverkehr ist es bedeutsam, dass in § 1 Abs. 1 Ziffer 9, „die Durchführung des bargeldlosen Zahlungsverkehrs und des Abrechnungsverkehrs (Girogeschäft)" ein Bankgeschäft darstellen und somit diese Tätigkeit ausschließlich von Kreditinstituten ausgeübt werden kann. Auch die Ausgabe und Verwaltung von elektronischem Geld (E-Geld-Geschäft) wird in § 1 Abs. 1 Ziffer 11 als Bankgeschäft definiert. Die Entscheidung, welche Unternehmen den Regelungen des KWG unterliegen, wird in § 4 KWG der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin) überlassen. Die BAFin übt gemäß § 6 Abs. 1 KWG die Aufsicht über die Institute nach den Vorschriften des KWG aus und „hat Mißständen im Kredit- und Finanzdienstleistungswesen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden, die ordnungsmäßige Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen oder erhebliche Nachteile für die

[87] Teil des Rechts gegen Wettbewerbsbeschränkungen ist ferner der EWG-Vertrag, der europäischem Wettbewerbsrecht für Deutschland zunehmende Bedeutung verleiht.
[88] Vgl. Herdzina (1993), S. 135.
[89] Lediglich die Teile 4 ff. des Gesetzes gelten, in denen die Vergabe öffentlicher Aufträge und Formalia geregelt werden.
[90] Gültig ist zur Zeit die Fassung des GWB aus 1998, deshalb ist die Bundesanstalt für Finanzdienstleistungsaufsicht noch nicht berücksichtigt.
[91] Vgl. Riehm (1998).
[92] 1. Abschnitt KWG.

Gesamtwirtschaft herbeiführen können“[93]. Zu diesem Zweck ist die BAFin gegenüber den beaufsichtigten Instituten anordnungsbefugt und mit einer Fülle an Kompetenzen ausgestattet.[94]

Die Bundesbank gilt nach § 2 Abs. 1 Ziffer 1 und Abs. 6 Ziffer 1 ausdrücklich nicht als Institut, das selbst unter die Regulierung nach KWG fällt. Die Struktur, Aufgaben und Kompetenzen der Bundesbank sind im Gesetz über die Deutsche Bundesbank festgelegt. Dieses gibt der Bundesbank weitreichende Kompetenzen, ihre Ziele zu erreichen. Die Ziele sind konform mit denen des Europäischen Systems der Zentralbanken (ESZB): unter anderem die Gewährleistung der Preisstabilität und die Sicherung der Abwicklung des Zahlungsverkehrs im Inland und mit dem Ausland und der Stabilität der nationalen Zahlungs- und Verrechnungssysteme.

Das Verhältnis von Deutscher Bundesbank und Bundesanstalt für Finanzdienstleistungsaufsicht im Sinne eines kooperativen Ansatzes wird im KWG § 7 festgelegt. Die laufende Überwachung der Institute ist Aufgabe der Bundesbank. Diese Überwachung umfasst neben der Überprüfung der Eigenkapitalausstattung und der Jahresabschlussunterlagen auch die Prüfung der Risikosteuerungsverfahren der Institute.[95] Die Bundesbank hat sich in ihrer Tätigkeit an den Richtlinien der BAFin zu orientieren. Diese sollten im Einvernehmen der beiden aufsichtlichen Institutionen erlassen werden; im Streitfall wird das Finanzministerium hinzugezogen. Die aufsichtsrechtlichen Maßnahmen wie Allgemeinverfügungen und Verwaltungsakte einschließlich Prüfungsanordnungen werden in § 7 Abs. 2 KWG von der BAFin im Einvernehmen mit der Bundesbank gegenüber den Instituten bestimmt. Die Erkenntnisse beider Institutionen sind laut § 7 Abs. 1, 3 und 4 KWG gegenseitig zur Verfügung zu stellen, eine informationstechnologische Verarbeitung auch personenbezogener erhobener Daten ist zulässig.

3.2.3 Ausgestaltungsmöglichkeiten der Bankenregulierung

Bankaufsichtliche Maßnahmen, Vorgaben und Normen lassen sich in verschiedene Kategorien einordnen (siehe Abbildung 6).

Während die einzelnen Ausprägungsformen der Regulierung an späterer Stelle ausführlich vertieft werden[96], ist an dieser Stelle von Bedeutung, dass die bankaufsichtlichen Optionen zur Marktregulierung vielfältig sind. Neben reinen Lösungen staatlicher Regulierung und privatwirtschaftlicher Selbstregulierung finden sich in Deutschland auch bemerkenswerte Ansätze kooperativer Regulierung, bei der hoheitliche Stellen und Privatwirtschaft im gemeinsamen Interesse einvernehmlich handeln und Standards und Abkommen festlegen. Das bekannteste Beispiel auf institutionalisierter Ebene ist der Zentrale Kreditausschuss (ZKA), in dem unter anderem die für den reibungslosen Ablauf des Zahlungsverkehrs wichtigen Zahlungsverkehrsabkommen ausgehandelt werden.

[93] § 6 Abs. 2 KWG.
[94] Vgl. im Detail KWG Dritter Abschnitt – Vorschriften über die Beaufsichtigung der Institute.
[95] § 7 Abs. 1 KWG.
[96] Siehe Kapitel 4 und 5.

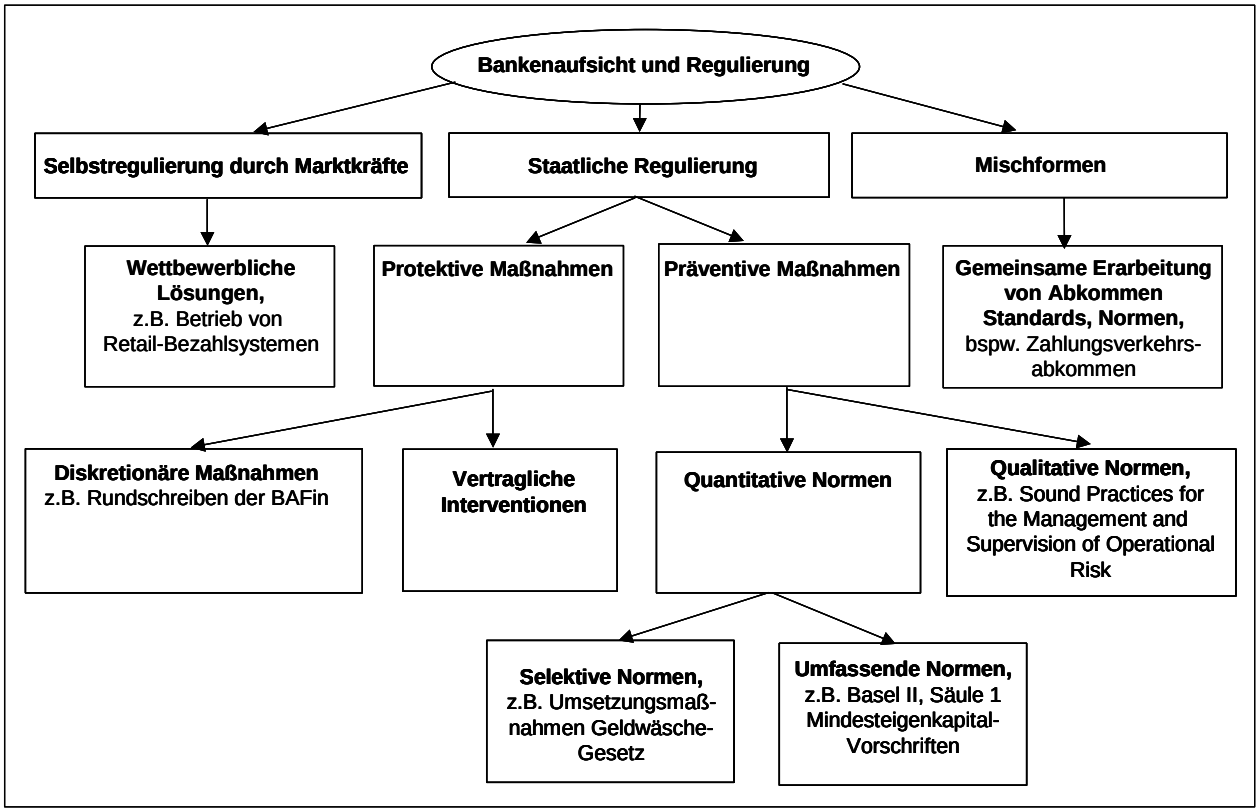

Abbildung 6: Strukturierung bankaufsichtlicher Maßnahmen, Vorgaben und Normen[97]

[97] In Anlehnung an Burghof (1996), S. 36, eigene Ergänzungen.

4 Elektronische Zahlungsverkehrslandschaft: Infrastruktur, Akteure und Regulierer

Die makroökonomische Bedeutung des Zahlungsverkehrs ist erheblich und kann über die Größenordnung der transferierten Beträge verdeutlicht werden. In Europa wurden im Jahr 2001 täglich fast 1.500 Mrd. Euro allein im Euro-Großzahlungsverkehr abgewickelt. Zum Vergleich: Das Bruttoinlandsprodukt der EU-15 betrug 2001 rund 9.000 Mrd. Euro.[98] Fabritius spricht in diesem Zusammenhang von sicheren Zahlungssystemen als *conditio sine qua non* sowohl für die Stabilität des Finanzsystems als auch für die reibungslose Durchführung der Geldpolitik in der Eurozone.[99]

Die Bestandszahlen an Zahlungsmitteln für Deutschland aufgeteilt nach Banken und Nicht-Banken (siehe Tabelle 1) vermitteln über ihre „geringe" absolute Höhe einen Eindruck, in welcher Größenordnung die Zahlungsverkehrssysteme in Anspruch genommen werden, wenn sie mit den Flussgrößen verglichen werden. In Deutschland wurden im Jahr 2000 allein im bargeldlosen Massenzahlungsverkehr Umsätze in Höhe von rund 30.636,5 Mrd. Euro getätigt.[100] Die Aufteilung auf die einzelnen Zahlungsverfahren zeigt Tabelle 2. Großzahlungsverkehr und Interbankenzahlungen, die ein Vielfaches dieser Werte (siehe Abschnitt 4.2.1) betragen, sind in diesen Zahlen nicht enthalten.

Zahlungsmittel von Nicht-Banken:	(in Mrd. Euro)
Umlauf von Bargeld (Banknoten und Münzen)	**125,1**
Aufladungswert in E-Geld-Systemen	**0,06**
Sichteinlagen	**448,7**
davon: Private Haushalte	268,7
Unternehmen	164,9
Sonstige	15,1
Zahlungsmittel von Banken	
Auf Zentralbankgeldkonten	**35,5**
davon: Mindestreserve	35,3
Überschussreserve	0,2
Sichteinlagen bei anderen Banken	**113,1**
nachrichtlich: Ausleihungen von der Zentralbank (Spitzenrefinanzierungsfazilitäten)	**0,6**

Tabelle 1: Bestandsgrößen – Zahlungsmittel in Deutschland (Banken und Nicht-Banken) im Jahr 2000[101]

[98] BIP der EU-15 2001: € 8.865,39 Mrd. (gerechnet in jeweiligen Preisen), SVR (2003), Tabelle 3*, S. 501.
[99] Fabritius (2001a), S. 3.
[100] Vgl. BdB (2003a).
[101] Jahresendstand. EZB (2002 f), Addendum, Germany und Deutsche Bundesbank (2003a), Tabelle 2 und Tabelle 3. Durch die Euroumstellung sind die Zahlen 2001, die im Februar 2003 verfügbar waren, deutlich abweichend von den Vorjahren, so dass an dieser Stelle auf das Jahr 2000 zurückgegriffen wird.

	Anzahl in Mio. Transaktionen		Wertvolumen in Mrd. Euro	
Überweisungen	**7.132,9**	**51,39 %**	**26.471,2**	**86,4 %**
Lastschriften	**5.532,1**	**39,85 %**	**3.065,0**	**10,0 %**
Schecks	**436,6**	**3,15 %**	**1.036,2**	**3,38 %**
Kreditkarten	**355,0**	**2,56 %**	**36,3**	**0,12 %**
electronic cash	**424,0**	**3,05 %**	**27,8**	**0,09 %**
Summe	**13880,6**	**100 %**	**30636,5**	**100 %**

Tabelle 2: Flussgrößen: Bargeldlose Transaktionen in Deutschland nach Anzahl und Wertvolumen im Jahr 2000 – Kundenzahlungen[102]

4.1 Dematerialisierung des Geldes und die Folgen

Die Geschichte des Zahlungsverkehrs ist eine Geschichte der Dematerialisierung des Geldes. Büschgen unterscheidet drei Dimensionen der Entwicklung des Zahlungsverkehrs:[103]

1) Es findet eine Transformation von Bargeld zu Buchgeld statt.
2) Das Trägermedium mit der Information „Geldwert" ist nicht länger papiergebunden, sondern elektronisch.
3) Die Zahlungsintermediäre sind zunehmend neben Banken auch Non- und Near-Banks.

Ad 1) Der zunehmende Einsatz von Giralgeld in der Breite der Bevölkerung hat seinen Anfang in Deutschland mit der Bereitstellung von kostenfreien Gehaltskonten in den fünfziger Jahren des 20. Jahrhunderts genommen. Die Rationalisierung der Lohn- und Gehaltszahlungen war ein Motiv der Unternehmen, die Bezahlung umzustellen, eine andere – die das kostenlose Führen der Konten rechtfertigte – war die Bindung der Kontenbesitzer an „ihre" Bank oder Sparkasse, die wiederum Cross-Selling-Effekte erhoffte. Zusätzlich konnten die Institute die Zinsspanne zwischen Einlagezins und Kreditzinsen gewinnbringend nutzen (Refinanzierungsfunktion).

Auf nationaler Ebene erarbeiteten die Finanzinstitute gemeinsam mit der Deutschen Bundesbank bis Anfang 1970 an einem einheitlichen Konzept zur Automatisierung von Zahlungen, die maschinell-optische Belegverarbeitung und der Datenträgeraustausch wurden somit möglich; auf internationaler Ebene wurde in den achtziger Jahren der EDIFACT-Standard (Electronic Data Interchange For Administration Commerce and Transport) geschaffen.

Ein Meilenstein aus der Perspektive der Sicherheit des Zahlungsverkehrs wurde Anfang 1980 mit der Vermarktung des RSA-Verschlüsselungsverfahrens (benannt nach den Initialen der Erfinder Rivest, Shamir und Adelman) möglich. Durch diese Verschlüsselungstechnik - im militärischen Umfeld wurden bereits zuvor andere Verfahren (u. a. DES) eingesetzt - wurde es möglich, in Informationsnetzwerken Daten sicher zu versenden, ohne den vorher üblichen hohen Aufwand der symmetrischen Verschlüsselungsverfahren beim Austausch und der Administration der geheimen Schlüssel.

[102] Vgl. BdB (2003a). Daten von EURO Kartensysteme, EUROCARD, eurocheque GmbH, Postbank und Bank für Internationalen Zahlungsausgleich. Ohne Großzahlungen und Interbankenzahlungsverkehr.
[103] Vgl. Büschgen (1998), S. 415 ff.

Der Individualverkehr Kunde-Bank wurde parallel automatisiert und individuelle Überweisungen, belegloser Scheckeinzug und zuletzt der elektronische Zahlungsverkehr Lastschriften realisiert – jeweils waren Abkommen im Zentralen Kreditausschuss für die gesamte Kreditwirtschaft erfolgreich verhandelt worden.

Eine weitere, parallel zu den vorherigen verlaufende, Stufe der Elektronisierung betraf die Verbindung Kunde-Handel-Bank am Point of Sale (POS). Mit der Akzeptanz von Debitkarten wie der ec-Karte, von Kreditkarten (seit den fünfziger Jahren) und von Kundenkarten (deren Anfänge in den USA in den dreißiger Jahren liegen), in den späten neunziger Jahren auch der GeldKarte, am Terminal der Händler wurde das Bezahlen im Alltag elektronisch möglich. In der Folge übertrifft das Transaktionsvolumen des bargeldlosen Zahlungsverkehrs eines Jahres mittlerweile – auf Privatkundenseite – den Umlauf an Bargeld (zum Jahresende) um das 240-fache).[104]

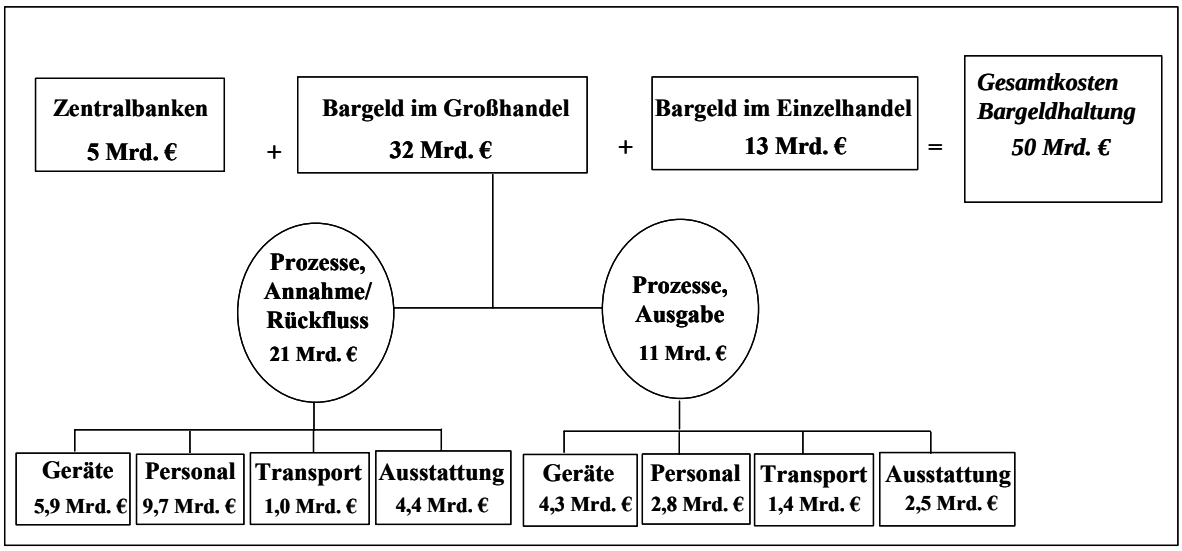

Abbildung 7: Kosten der Bargeldhaltung in der EU pro Jahr[105]

Die Kosten der Bargeldhaltung liefern eine zusätzliche Motivation für die Umstellung von Bargeld auf elektronische Zahlungssysteme. Die Arbeitsgruppe „Cash" des European Payments Council (EPC) schätzt die Kosten der Bargeldhaltung in der Europäischen Union auf eine Summe von € 50 Mrd. pro Jahr (siehe Abbildung 7). Dazu kommen noch die Kosten der Banken selbst für die Bargeldversorgung. Allein für Deutschland, schätzt die Arbeitsgruppe „Cash", belaufen sich diese Zahlen auf € 9 Mrd. unter der Annahme, dass bei 45.000 Zweigstellen jeder Filiale € 200.000 an Kosten für Bargeldhandling p.a. entstehen.[106] Die Infrastrukturkosten für Buchgeldtransfers sind dem jedoch nicht gegenübergestellt. Eine erste Annäherung an diese Ausgaben erhält man durch die Kosten, die für die Entwicklung bis zur Produktion von STEP2[107] auf die beteiligten Banken und die Betreibergesellschaft der Euro Banking Association (EBA) zugekommen sind: 10 Mio. €.[108] Diese auf den ersten Blick

[104] Siehe auch Tabelle 1 und Tabelle 2.
[105] BdB (2003b), S. 78 basierend auf Grundlage von Arbeitsunterlagen der EPC Arbeitsgruppe „Cash". Leicht modifizierte eigene Darstellung. Leider stehen keine Kostenannahmen für die zusätzlichen Kosten der Geschäftsbanken für die Bargeldbereitstellung in Europa zur Verfügung.
[106] Vgl. BdB (2003b), S. 77. Aus Sicht des Autors scheint diese Zahl sehr hoch gegriffen, in Ermangelung besserer Zahlen wird sie an dieser Stelle dennoch genannt.
[107] Das einzige paneuropäische Massenzahlungssystem, siehe ausführlich 4.2.3.5.4.
[108] o.V. (2003d). Unberücksichtigt sind bei der Kostenrechnung die bestehenden Infrastrukturen, auf denen STEP2 aufbaut.

niedrig anmutende Summe berücksichtigt allerdings noch nicht die vorhandene Infrastruktur der Zahlungssysteme, an die STEP2 andockt, und deren Kosten. Darüber sind keine Angaben bekannt.

Ad 2 und 3) Bereits 1918 wurde erstmals in den USA Geld elekronisch per Telegraph von einer Federal Reserve Bank transferiert. Gleichwohl dauerte es bis in die siebziger Jahre des 20. Jahrhunderts bis sich mit automatisierten Clearingstellen (in den USA Automated Clearing House (ACH)) eine elektronische Alternative zur papiergebundenen Scheckverarbeitung im Geschäftsleben durchsetzen konnte.[109]

Die zunehmende Abwicklung der Zahlungstransaktionen in elektronischer Form hat neben den Finanzinstituten den Markt auch für andere Dienstleister attraktiv werden lassen. In Deutschland ist zwar die Durchführung des bargeldlosen Zahlungsverkehrs und des Abrechnungsverkehrs (Girogeschäft) gemäß Kreditwesengesetz (KWG) ein beaufsichtigungspflichtiges Bankgeschäft.[110] Somit können nur Kreditinstitute, die durch das KWG als solche definiert werden, wenn sie eines oder mehrere der in § 1 Abs. 1 aufgeführten Bankgeschäfte erledigen, diese Aufgaben wahrnehmen. Anbieter technischer Dienstleistungen, Non- und Near-Banks haben in den letzten 30 Jahren gleichwohl zunehmend Bereiche der Wertschöpfung erobert, die vormals der Finanzwirtschaft vorbehalten waren. Teilweise sind diese Dienstleistungen an der Grenze zu bankerlaubnispflichtigen Geschäften, und nur mit detaillierten Vertragsklauseln in Abstimmung mit der Bundesanstalt für Finanzdienstleistungsaufsicht zulässig. Beispielsweise bietet die Bibit Internetzahlungen GmbH, Tochter der niederländischen Bibit B.V., Händlern an, (weltweite) Zahlungsvorgänge, die aus unterschiedlichen Verkaufskanälen stammen, über eine Internet-Infrastruktur abzuwickeln.[111] Verkaufskanäle sind üblicherweise Webshops, Call-Center oder POS-Terminals. Bibit funktioniert dabei als integrierender Dienstleister, der 60 internationale Zahlungsmethoden in unterschiedlichen Währungen digital vereinheitlicht.

Ein Teil der durch die Elektronisierung ermöglichten Rationalisierungsgewinne ist in der Folge dieser Tendenz von Dienstleistern abgeschöpft worden. Der steigende Wettbewerb führt zur zunehmenden Realisierung von Skaleneffekten durch Konzentration und Kooperation im Back-Office-Bereich der Banken. Die Entwicklung von Transaktionsbanken, die den Zahlungsverkehr oder die Wertpapierabwicklung für ein Konsortium von Banken abwickeln können, steht erst am Anfang. Noch ist nicht entschieden, inwieweit bestimmte Bereiche im Transaktionsbankenangebot ebenfalls von dritten Dienstleistern übernommen werden können.

4.2 Nationale und supranationale Bankennetze

Der Zahlungsverkehr lässt sich in den Inlands- und Auslandszahlungsverkehr unterteilen. Für beide Arten stehen unterschiedliche Infrastrukturen zur Verfügung, die ineinander übergreifen. Das Verhältnis von Inlandszahlungsverkehr zu grenzüberschreitendem Zahlungsverkehr lag in Deutschland 2001 bei ungefähr 99:1.[112] Die Größenordnung des europäischen Zahlungsverkehrs in Deutschland reduziert sich weiter auf 0,5 % am gesamten deutschen Zahlungsverkehr, die anderen 0,5 % sind Zahlungen aus Deutschland ins nicht-europäische Ausland.[113]

[109] Vgl. Frey (2003).
[110] KWG § 1 Abs. 1 und weitere Ausführungen Riedl (2002), S. 31.
[111] www.bibit.com.
[112] Rehm (2001), S. 5.
[113] BdB (2003b), S. 13.

Die Infrastruktur über die alle Zahlungen abgewickelt werden, besteht aus nationalen und supranationalen Banknetzen.

Es lassen sich bei den nationalen Banknetzen zwei Anbietergruppierungen unterscheiden, über die Zahlungen abgewickelt werden können. Die Deutsche Bundesbank bietet als hoheitlicher Betreiber Dienstleistungen im Zahlungsverkehr an. Die privaten Anbieter – Geschäftsbanken, Zahlungssystemanbieter, Netzbetreiber – bilden die zweite Kategorie. Eingebunden sind die nationalen Zahlungsnetze in den europäischen und in den internationalen Kontext, wie im folgenden dargelegt wird.

Die Gestaltung der Zahlungsnetze, die zuständigen Betreiber und der Grad der staatlichen Intervention waren und sind international und europäisch durchaus unterschiedlich ausgeprägt. Im Rahmen der vorliegenden Arbeit wird exemplarisch für die nationale Gestaltung des Zahlungsverkehrs die Bundesrepublik Deutschland mit ihren Außenbezügen betrachtet. Diese Beschränkung erscheint angesichts des hohen Anteils Deutschlands am europäischen Zahlungsverkehr gerechtfertigt, zumal in Deutschland durch den parallelen Betrieb privater und staatlicher Netze eine umfassende Darstellung möglicher Bezahlsystemvarianten gelingt.

4.2.1 Banken- und Zahlungsverkehrsinfrastruktur in Deutschland

2003, nach der tiefgreifenden Strukturveränderung in der Folge des 7. Gesetzes zur Änderung des Gesetzes über die Deutsche Bundesbank, umfasst die Deutsche Bundesbank neun Hauptverwaltungen mit 66 nachgeordneten Filialen (vormals Hauptstellen) in größeren Städten.[114] In Deutschland gab es Ende 2001 2.696 Kreditinstitute mit 53.931 Zweigstellen, darunter 303 Kreditbanken, 547 Sparkassen und Landesbanken und 1.623 genossenschaftlich geführte Banken.[115] Insgesamt wurden an diesen Banken Ende 2001 ca. 87 Millionen Girokonten geführt, bereits 19 Millionen davon online – Tendenz weiter steigend.[116]

In Deutschland standen 2002 nach Angaben des Bundesverbandes deutscher Banken 50.487 Geldautomaten[117]. Die Anzahl an Karten mit Debitkartenfunktion lag 2001 bei 115 Mio., hinzu kamen knapp 19 Mio. Kreditkarten. Die Zahl der Akzeptanzstellen für Kreditkarten lag 2001 bei 1.338.221, allerdings werden mögliche Doppelzählungen von der Bundesbank nicht ausgeschlossen, da die Angaben auf die Kreditkartengesellschaften zurückgehen – und eine unbestimmte Zahl von Akzeptanzstellen Kreditkarten verschiedener Organisationen annimmt. Für Debitkarten wurden 435.680 Akzeptanzstellen gemeldet.[118]

Die Anzahl der inländischen Transaktionen, im Massenzahlungsverkehr fast 2,2 Mrd., die von der Deutschen Bundesbank 2001 als Betreiberin ausgewählter Interbankenzahlungssysteme abgewickelt wurden, vermittelt ein Gespür für die Dimensionen im Zahlungsverkehr. Demgegenüber wurden im Individualzahlungsverkehr (Brutto- und Nettoabwicklungssysteme für Großzahlungen) im gleichen Zeitraum 31,1 Mio. Transaktionen abgewickelt. Dabei ist die Werthaltigkeit der Transaktionen sehr unterschiedlich: Die Kleinzahlungsbeträge summierten sich 2001 auf 2.202,3 Mrd. Euro mit einer durchschnittlichen Transaktionshöhe von circa

[114] Bis zum 31.3.2003 wurden 20 Filialen (19 vormalige Zweigstellen und eine Hauptstelle) geschlossen. Weitere 32 vormalige Zweigstellen werden in Betriebsstellen fast ohne Außenbetrieb (Beschränkung auf Abwicklung des Barzahlungsverkehrs mit Großkunden) umgewandelt und bis spätestens 30.4.2007 geschlossen. Vgl. Deutsche Bundesbank (2002a), Folie 67.
[115] Deutsche Bundesbank (2003c), S. 104.
[116] Deutsche Bundesbank (2003a), S. 6.
[117] BdB, www.bdb.de/download/statistik-service/1-3-3-1-Kartengestuetzter_Zahlungsverkehr.pdf, basierend auf Angaben des ZKA.
[118] Deutsche Bundesbank (2003a), S. 6.

1.000 Euro, die Großzahlungen hingegen auf 70.472,2 Mrd. Euro mit durchschnittlich 2,27 Mio. Euro pro Transaktion.[119]

Der inländische Zahlungsverkehr wird mit Hilfe von Gironetzen (siehe Abbildung 8).gewährleistet, die von den großen Bankengruppen und der Deutschen Bundesbank betrieben werden

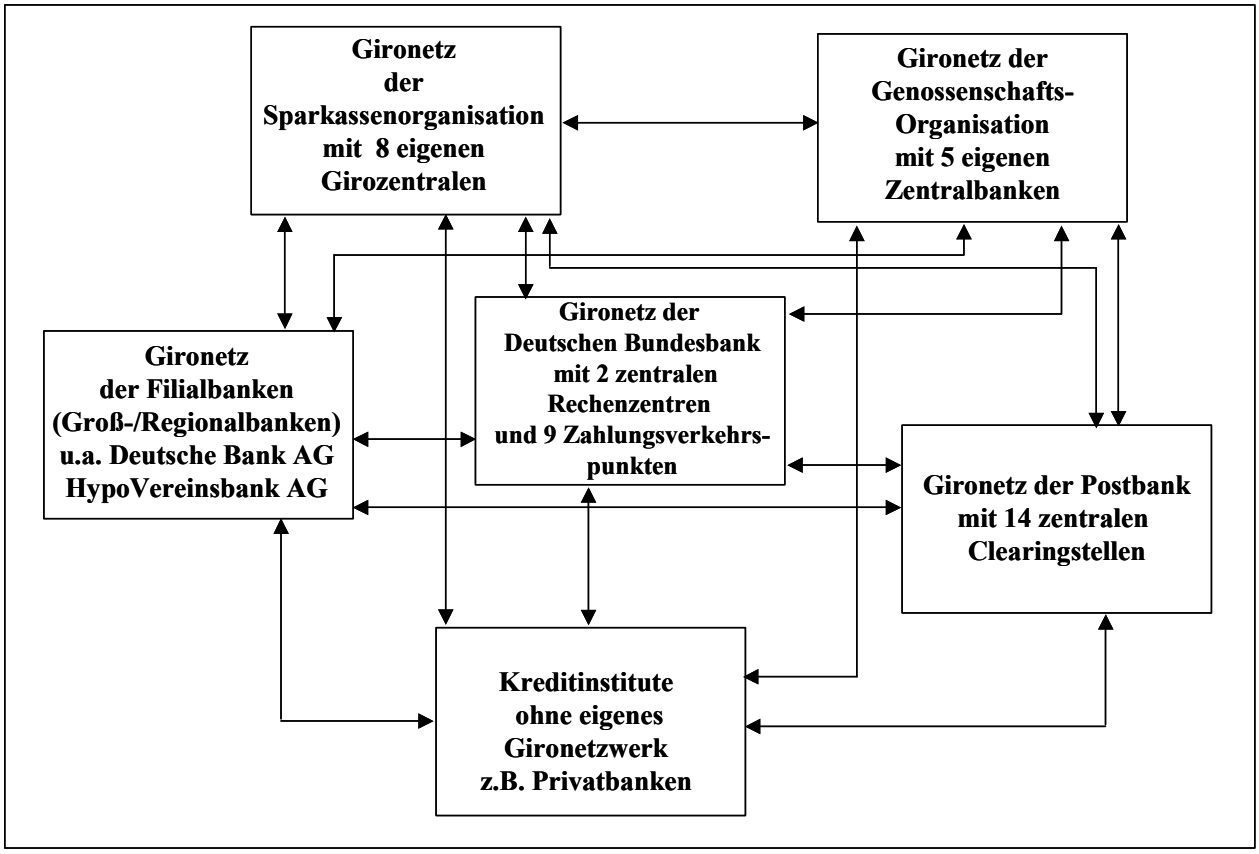

Abbildung 8: Verbindungen innerhalb der deutschen Gironetze[120]

Die Institutsgruppen mit großem Transaktionsvolumen betreiben jeweils eigene Zahlungsverkehrs-Infrastrukturen. Neben der Zentralbank sind dies die Sparkassen mit ihren Girozentralen, die Genossenschaftsbanken mit ihren Zentralstellen, die privaten Großbanken sowie die Postbankgruppe. Ein Auftrag innerhalb einer Institutsgruppe verbleibt in der Regel im eigenen, hierarchisch aufgebauten Verrechnungsnetz und wird nur bis zum nächsten von beiden Parteien erreichbaren Netzknoten durchgereicht. In der Hierarchie sind die jeweiligen Zentralstellen (u.a. die Zentralbank der Genossenschaftsorganisation und die Girozentralen der Sparkassenorganisation) die oberste interne Verrechnungsstufe, an die jeweils die Filialen direkt oder indirekt angeschlossen sind. Die einzelnen Institutsgruppen sind jeweils unmittelbar miteinander verbunden und unterhalten zusätzlich regional direkte Verbindungen; teilweise bestehen auch institutsübergreifende Verbindungen, die auf einzelne Relationen, zwischen denen ein hohes Transaktionsvolumen auftritt, beschränkt sind. So können beispielsweise lokale oder regionale Kooperationen zwischen Rechenzentren der Sparkassen und der Volksbanken dazu führen, dass der Weg über die Zentralinstitute gespart werden kann.

[119] Deutsche Bundesbank (2003a), Tabellen 7 und 8.
[120] EZB (2001a), S. 131, Riedl (2002), S. 41.

Mit dem Gironetz der Deutschen Bundesbank sind alle rechtlich eigenständigen Kreditinstitute unmittelbar verbunden, da sie gesetzlich verpflichtet sind, ein Zentralbankkonto bei der Bundesbank in Frankfurt, ihren Hauptverwaltungen oder ihren Filialen zu unterhalten.[121] Jedes beliebige Konto in Deutschland kann über diese Infrastruktur per Buchung angesprochen werden.

Ein Zahlungsvorgang läuft im Allgemeinen wie folgt ab: Die lokalen Kreditinstitute und Sparkassen erhalten die zahlungsrelevanten Daten in beleghafter oder elektronischer Form (durch günstigere Preise für den Endkunden aber auch für die Finanzinstitute bei der Deutschen Bundesbank wird versucht, die beleglose elektronische Form einheitlich durchzusetzen). Die Banken reichen die Zahlungsaufträge (Scheck, Lastschrift, Überweisung) an das jeweils zu ihrem Netz gehörende Rechenzentrum. Betreiber der Rechenzentren sind in der Regel die jeweiligen Dachorganisationen, denen ein Kreditinstitut angehört. Die Sparkassen beispielsweise betreiben drei Rechenzentren, vor wenigen Jahren lag die Zahl noch bei zehn. Die hauseigenen Rechenzentren transferieren die Daten in vorgegebenen Formaten an die zuständigen Clearing-Häuser/Transaktionsbanken, die regional das Clearing als Dienstleistung für die Institutsgruppen übernehmen und die Daten zu den Zentralinstituten weiterleiten.

Das Clearing der Zahlungsinformationen auf nationaler Ebene kann wahlweise über die jeweiligen Zentralinstitute oder deren Rechenzentren im eigenen Netz geschehen oder es kann auch vom Zentralinstitut der Weg ins Bundesbanknetz gewählt werden. Der Verrechnungsweg der verechneten Zahlungsdaten retour geht genau entgegengesetzt vom Bundesbanknetz zum regional zuständigen Zentralinstitut und von dort über das Konto des Kreditinstituts beim Zentralinstitut zurück auf die lokale Ebene.

Je nach Anbindung der involvierten Institute oder Filialen ist die Zahlungskette mehr oder weniger kurz, mit entsprechenden Folgen für den Verarbeitungsaufwand und die Transaktionsdauer. Die grundsätzliche Taktik der jeweiligen Institute besteht in dem Versuch, Haben-Positionen möglichst lange im eigenen Netz zu behalten und die Soll-Positionen schnell weiter zu reichen.[122] Die gesetzlichen Grundlagen haben diesen Versuchen jedoch einen engen zeitlichen Rahmen gesetzt: eine Überweisung darf in Deutschland nach § 676a Abs. 2 Bürgerliches Gesetzbuch seit 1.1.2002 nur noch maximal 3 Tage im Bankennetz verbleiben; innerhalb einer Haupt- oder einer Zweigstelle eines Kreditinstituts muss die Gutschrift sogar innerhalb eines Banktags erfolgen, andere institutsinterne Überweisungsaufträge dürfen längstens zwei Banktage dauern. Die Gesetzgebung wurde 1999 durch das Überweisungsgesetz geändert, welches in Folge der Richtlinie der Europäischen Union 97/5/EG vom 27.2.1997 (EU-Überweisungsrichtlinie) erforderlich wurde. Die Richtlinie regelt noch einige andere Einzelheiten im Bereich grenzüberschreitender Überweisungen, aber auch Inlandszahlungen im Sinne des Verbraucherschutzes.[123]

Für Retail-Zahlungen hat sich ein Verfahren eingebürgert, das unter dem Namen „Garagen Clearing“ bekannt ist.[124] Es bedeutet im Kern, dass die Informationen über Zahlungen bei den Zentral- oder Kopfstellen der Gironetze der Geschäftsbanken bilateral ausgetauscht werden. Der finale Zahlungsausgleich erfolgt direkt über das Gironetz der Deutschen Bundesbank und die entsprechenden Institutskonten. Die Bedeutung der Deutschen Bundesbank im Massenzahlungsverkehr hat in den letzten Jahren tendenziell abgenommen, da das Garagen-Clearing

[121] Vgl. § 19 Abs. 1 ESZB-Satzung.
[122] Vgl. z. B. EZB (2001a), S. 136f.
[123] Vgl. ausführlich Hartmann (1999).
[124] Vgl. EZB (2001), S. 136.

stetig zugenommen hat. Fabritius spricht von einer Halbierung des Anteils der Deutschen Bundesbank bei der Abwicklung des Massenzahlungsverkehrs innerhalb des letzten Jahrzehnts von 30 % auf 15 %.[125] Die Deutsche Bundesbank möchte dem entgegenwirken und überlegt, selbst am Garagen-Clearing, quasi als Kopfstelle insbesondere auch kleinerer Finanzinstitute, mitzuwirken.[126]

Die Verbindungen zwischen den Kreditinstituten, zu den Hauptstellen und Filialen der Deutschen Bundesbank, de facto zu deren Rechenzentren, laufen soweit es das Datenaufkommen und die zugrundeliegende Infrastruktur zulassen über eigene Kommunikationswege; die Daten gehen nicht über öffentliche Telekommunikationsleitungen. Die Rechenzentren mieten beispielsweise eigene Leitungen von den Telekommunikationsdienstleistern. Somit ist aus Sicht kritischer Infrastrukturen ein Angriff auf öffentliche Telekommunikationseinrichtungen indirekt auch ein Angriff auf die Zahlungsverkehrsnetze. Die entsprechenden Kabel insbesondere in und aus den Rechenzentren verlaufen in der Regel nicht in einem Strang, sondern werden bewusst an verschiedenen Orten verlegt, nicht in erster Linie wegen vermuteter gezielter Sabotage, vielmehr wegen Pannen bei Bauarbeiten.

Der Datentransport wird über speziell entwickelte einheitliche Software (z. B. Connect: Direct™ [127] und Direct Connect) abgewickelt, die auf bewährte kryptographische Verfahren zurückgreift. Ziel ist es, Unterbrechungen oder Manipulationen während der Datenübertragung feststellen zu können. Bei den Rechenzentren werden an unterschiedlichen Lokationen vollständige Backups angelegt. Sollten Daten manipuliert worden sein oder Systemfehler auftreten, kann der Zustand ex ante möglichst rasch wieder herbeigeführt werden, und eine meist händische Nachbearbeitung die Lücken bis zur letzten Sicherungskopie auffüllen. Fachleute in den Rechenzentren bezweifeln, dass Außentäter mit abgefangenen Zahlungs-Daten aus den Rechenzentren, die sie erst einmal als solche identifizieren müssten, tatsächlich Schaden verursachen könnten. Lediglich in Kombination mit Innenkenntnissen lassen sich Bedrohungspotenziale aufzeigen. Die Wiederherstellung von Transaktionsdaten bei Großzahlungen ist im Bundesbanknetz und in vergleichbaren Netzen anderer europäischer Länder bereits vorgekommen, und angesichts der im Vergleich zu den Massenzahlungen überschaubaren Anzahl an Transaktionen auch verhältnismäßig einfach.

Zum Zweck einheitlicher Standards bei der Datenübertragung gibt es wiederum Arbeitskreise und entsprechende Normungsgremien der Rechenzentren einzelner Verbände und übergeordneter Ebenen, teils unter Mitwirkung des Zentralen Kreditausschusses (ZKA).

Die Verrechnungswege für alle anderen Zahlungsarten sind analog zu den oben dargestellten zu sehen. Die Verarbeitung von Buchungen von Geldausgabeautomaten (ATMs) ebenso wie Kreditkartenzahlungen oder andere Point-of-Sale-Zahlungen (POS) geschieht mit Hilfe von Überweisungen und Lastschriften. Es wird in den Zentralinstituten oder den Clearing-Häusern verarbeitet, und es werden entsprechende Überweisungen und Lastschriften generiert. Beispielsweise löst eine ATM-Abhebung eine Lastschrift beim Konto des Kunden aus und eine Überweisung an das den Geldautomaten betreibende Kreditinstitut.

Visa und MasterCard betreiben die weltweit größten Kreditkartennetze. Es handelt sich im eigentlichen Wortsinn nicht um eigene Netze, sondern um die Anzahl geworbener Händler und Banken, die diese Kreditkarten akzeptieren und die technisch in die Lage versetzt werden, mit den jeweiligen Knotenpunkten zu kommunizieren. Die eigentliche Leistung der Kredit-

[125] Fabritius (2001), S. 13 f.
[126] Vgl. Friederich (2001), S. 3 f.
[127] www.stercomm.de.

kartenorganisationen besteht darin, in nationalen und internationalen Verträgen mit den Kartenherausgebern und -akzeptanten ein homogenes Netzwerk geschaffen zu haben, das trotz großer regionaler Unterschiede in der technischen Infrastruktur und Zahlungskultur, die weltweite Durchleitung und Verarbeitung einer Zahlung ermöglicht. Die Verträge mit den jeweiligen Händlern berücksichtigen neben Haftungsfragen und der Preisgestaltung auch die jeweilige Anbindung der Vertriebsstrukturen der Kartenherausgeber und -akzeptanzstellen.

In Deutschland betreiben vier Gesellschaften Debitkartennetze, auch EFTPOS (Electronic Funds Transfer at the Point of Sale) genannt. Alle Betreiber unterliegen den länderspezifischen Anforderungen des ZKA an externe Netzbetreiber.

Für bestimmte Dienstleistungen wie beispielsweise Kartenzahlungen, Wertpapierabwicklung und Devisentransaktionen gibt es spezialisierte Abwicklungskanäle und Bankendienstleister (mit verschiedenen Finanzinstituten als Eigner) wie die Gesellschaft für Zahlungssysteme (GZS)[128], welche die Kreditkartenabwicklung für verschiedene Kreditinstitute und große Handelsketten betreibt und 2002 mehr als 800 Mio. Transaktionen im Debit- und Kreditkarten-Zahlungsverkehr abgewickelt hat.

Im Bereich der Devisentransaktionen – weltweit werden täglich über $ 2.000 Mrd. an Fremdwährungsgeschäften durchgeführt – setzt seit September 2003 die in New York angesiedelte CLS-Bank (Continiuous Linked Settlement) neue Maßstäbe bei Effizienzsteigerungen und der Minimierung des Erfüllungsrisikos[129] im Devisenhandel. Die CLS-Bank rechnet bis 2004 mit einer Steigerung der Transaktionen um 150 %.[130]

4.2.2 Dienstleistungsangebot der Deutschen Bundesbank im unbaren Zahlungsverkehr

Die Deutsche Bundesbank hat laut Artikel 3 der Satzung des ESZB und der EZB den Auftrag, das reibungslose Funktionieren der Zahlungssysteme zu fördern. Laut § 3 Bundesbankgesetz hat die Deutsche Bundesbank für die bankmäßige Abwicklung des Zahlungsverkehrs im Inland und mit dem Ausland zu sorgen („Sorge-Auftrag“[131]) und zur Stabilität der Zahlungs- und Rechnungssysteme beizutragen. Dafür stellt die Bundesbank den Kreditinstituten der verschiedenen Bankengruppen ein wettbewerbsneutrales Gironetz zur Verfügung.[132] Dieses können Girokonteninhaber der Deutschen Bundesbank nutzen. Die Infrastruktur der Bundesbank beinhaltet neben dem Netz der Hauptverwaltungen und Filialen zu diesem Zweck 7 Rechenzentren und 2 Zahlungsverkehrspunkte (Stand Februar 2003).

Der unbare Zahlungsverkehr wird in Individualzahlungsverkehr (Großzahlungsverkehr) und Massenzahlungsverkehr (Retail-Zahlungsverkehr) unterschieden. Den Großzahlungsbereich zeichnen hohe Beträge, in der Regel deutlich über € 10.000, aus. Eine klare Betragsgrenze gibt es jedoch nicht, beispielsweise liegt beim Großbetrag-Scheckeinzug die Grenze bereits bei € 3000. Für darunter liegende Beträge ist der Massenzahlungsverkehr zuständig.

Für grenzüberschreitende Zahlungen per Deutscher Bundesbank im Individualzahlungsverkehr sind der Zugang zu TARGET[133], oder in Zukunft die Weiterentwicklung TARGET2[134],

---

[128] Vgl. www.gzs.de.
[129] Bekanntes Beispiel für ein solches Risiko ist die Herstatt-Bank, die in den siebziger Jahren Auslöser einer systemischen Krise im Devisenhandel war; mit der Folge, dass heute der Begriff Herstatt-Risiko diese Risikoart beschreibt.
[130] Vgl. www.cls-group.com.
[131] Stark (2001), S. 4.
[132] Vgl. Darstellung der Bundesbank im Internet, www.bundesbank.de.
[133] Vgl. ausführlich 4.2.3.3.

und der Auslandszahlungsverkehr (AZV) geeignet. Der Massenzahlungsverkehr ins Ausland ist bei der Bundesbank bislang beschränkt auf Auslandsanweisungen öffentlicher Kassen, beispielsweise Rentenauszahlungen.

4.2.2.1 Angebot der Deutschen Bundesbank im Individualzahlungsverkehr

Im Individualzahlungsverkehr, auch Großzahlungsverkehr genannt, werden sogenannte Brutto- und Nettoabwicklungssysteme unterschieden, abhängig von der Verarbeitung und dem Zahlungsausgleich. Während bei Bruttosystemen jede Transaktion ohne Aufschub (bei Echtzeit-Systemen sofort) verarbeitet wird, wird bei Nettosystemen nur die Differenz der Soll- und Habenpositionen gesettlet, das heißt die Zahlungsverpflichtungen ausgeglichen.

Bruttoabwicklungssysteme:
- Elektronischer Schalter (ELS) bis Ende 2004
- RTGS^{plus}

(Nettoabwicklungssysteme:
- Elektronische Abwicklung Frankfurt (EAF) bis 5.11.2001)

4.2.2.1.1 RTGS^{plus}

Hintergrund der notwendig gewordenen Entwicklung von RTGS^{plus} war ein verschärfter Wettbewerb der Euro-Zahlungssysteme im Rahmen der Euro-Einführung. Dieser halbierte bis Ende 1999 Umsätze und Volumen der über EAF abgewickelten Zahlungen im Vergleich zur Phase vor der Euroeinführung.[135] RTGS^{plus} führte die Systeme EAF und ELS (siehe 4.2.2.1.2 und 4.2.2.1.3) zu einem neuen wettbewerbsfähigen System zusammen.

Im Ergebnis ist RTGS^{plus} ein Bruttosystem mit liquiditätssparenden Elementen, das die Funktion des deutschen TARGET-Zugangs übernommen hat. Ein Vorteil für die Teilnehmer ist die umfangreiche Möglichkeit, die Zahlungsabwicklung je nach Durchsatz und Liquiditätserfordernissen selbst zu gestalten. Die Einführung liquiditätssparender Algorithmen (neue Verfahren zur Warteschlangenauflösung bei nicht genügender Liquidität) ist in dieser Form in RTGS-Systemen neu.[136] Mit Limit-Zahlungen und der „Liquiditätsbrücke“[137] können die Teilnehmer ihre Liquidität weiter steuern (im Gegensatz zu Nettosystemen, in denen Limits als Risikobegrenzung notwendig werden). Die Liquiditätssteuerung wird zunehmend zum betriebswirtschaftlichen Steuerungsinstrument. Die Bundesbank berichtet von Geschäftsbanken, die Innertagesliquidität intern mit 15 bis 20 Basispunkten bepreisen.[138]

Als Kommunikationsplattform für den Zahlungs- und Informationsaustausch zwischen den direkten Teilnehmern und RTGS^{plus} dienen die von SWIFT bereitgestellten internationalen Standards und Services – ein im nationalen Zahlungsverkehr bisher unübliches Prinzip. Die Zahlungsabwicklung läuft über den für die Kommunikation von Echtzeit-Bruttosystemen und Teilnehmern speziell entwickelten SWIFT-Y-Copy-Service[139], über den Zahlungen in den

---

[134] Vgl. ausführlich 4.2.3.4.
[135] Vgl. Deutsche Bundesbank (2000a), S. 65 f.
[136] Vgl. Deutsche Bundesbank (2000a), S. 69 f.
[137] Das Innertageskonto einer Bank als Teilnehmer bei RTGS^{plus} wird mit einem bei der Heimat-Zentralbank geführten beliebigen Konto verbunden. Liquidität kann zwischen den Konten während des Tages transferiert werden. Vgl. Deutsche Bundesbank (2000), S. 63.
[138] Vgl. Deutsche Bundesbank (2000), S. 62. Die absolute Höhe dürfte sich nach dem jeweils aktuellen Zinsniveau richten.
[139] Generell wird der FIN Copy Dienst in SWIFT genutzt, um eine Kopie einer Zahlungsnachricht an ein System zu schicken, um die Authorisierung für eine Fortsetzung der Bezahltransaktion zu erhalten.

gängigen MT-Formaten (MT 103/MT 202) eingereicht werden können. Über einen neuen SWIFTNet InterAct Service können die Teilnehmer sich entweder online mittels XML-Nachrichtentypen (Extensible Markup Language) über den Stand der Zahlungen informieren und interaktiv eingreifen oder über einen weiteren SWIFT-Dienst, SWIFT Alliance Webstation und SWIFTNet InterAct Browse per Dialog auf alle relevanten Daten zugreifen.[140]

Auf der Kostenseite ist hervorzuheben, dass RTGS^{plus} als das erste Zahlungssystem im Individualzahlungsverkehr bezeichnet wird, welches mittels der erhobenen Transaktionskosten kostendeckend ohne Quersubventionierung arbeiten soll.[141] RTGS^{plus} kann aus Sicht der Deutschen Bundesbank bislang als Erfolg gefeiert werden. Es ist das größte Settlement-System der Europäischen Union. Pro Arbeitstag werden im Schnitt ca. 140.000 Zahlungen bearbeitet, die einen Wert von fast € 600 Mrd. haben; das Verhältnis von Inlands- zu Auslandszahlungen lag zahlenmäßig bei 6:1, wertmäßig bei 2,7:1.[142] Bereits 60 % aller Zahlungen sind Kundenaufträge. Über die Hälfte der Aufträge liegt unter € 12.500. Anfang 2003 lag der Anteil der Großbetrags-Zahlungen (Stückzahlen), die europaweit abgewickelt wurden, für RTGS^{plus} bei 30%, grenzüberschreitende Zahlungen wurden zu 50 % von RTGS^{plus} abgewickelt. Dabei werden fast 80 % der Express-Zahlungen innerhalb einer Sekunde verarbeitet, und rund 80 % der Limit-Zahlungen (mit denen das Vorleistungsrisiko gesenkt werden kann) werden binnen 10 Sekunden durchgeleitet.

Die Anzahl der direkten Teilnehmer ist bis Mitte 2003 auf 76 gestiegen, über 9.000 Kreditinstitute können europaweit mit dem System unmittelbar erreicht werden. Kreditinstitute können auch indirekt über einen frei zu wählenden direkten RTGS^{plus}-Teilnehmer am Verfahren partizipieren, beispielsweise ist die Bundesbank nicht nur Betreiberin des Systems, sondern auch direkter Teilnehmer. Somit können alle Inhaber eines Kontos bei der Deutschen Bundesbank indirekt auf RTGS^{plus} zugreifen.

Die Weiterentwicklung von RTGS^{plus} hängt maßgeblich von der Einigung der europäischen Zentralbanken ab, TARGET2[143] zu positionieren. Aufgrund der starken Stellung von RTGS^{plus} innerhalb TARGET kann jedoch von einer bedeutenden Einflussmöglichkeit der Deutschen Bundesbank in diesem Prozess ausgegangen werden.

4.2.2.1.2 Elektronischer Schalter

Der Elektronische Schalter, auch Euro Link System (ELS) genannt, ist (ebenso wie die in RTGS^{plus} aufgegangene Elektronische Abwicklung Frankfurt (EAF)) ein Interbanken-Verfahren zur nationalen und weltweiten Abwicklung von Euro-Zahlungen. Das Verfahren garantiert fortlaufend endgültige Zahlungen sowie Verrechnung in Zentralbankgeld innerhalb eines Geschäftstages.

ELS ist der deutsche Zugangspunkt zu TARGET[144] für die Kreditinstitute, die (noch) nicht über einen Zugang zu RTGS^{plus} verfügen. Mit der Einführung des neuen Echtzeit-Bruttozahlungssystem RTGS^{plus} im November 2001 hat ELS erheblich an Bedeutung verloren. Der Übergang auf RTGS^{plus} soll der Kreditwirtschaft erleichtert werden, daher wird

[140] Vgl. Deutsche Bundesbank (2001a).
[141] Vgl. Fabritius (2001), S. 13.
[142] Alle Zahlen (teils eigene Berechnung) auf Grundlage von BdB (2003b), S. 38f und Deutsche Bundesbank (2002d).
[143] Die Weiterentwicklung und Harmonisierung des aktuellen europäischen Verbund-Großzahlungssystems, über das das Settlement der Zahlungen läuft (vgl. ausführlich 4.2.3.3 und 4.2.3.4).
[144] Das europäische Verbund-Großzahlungssystem, über das das Settlement der Zahlungen läuft (vgl. 4.2.3.3).

ELS noch bis 2004 weiterbetrieben. Das Bundesbanksystem ermöglicht es den Instituten, Empfänger außerhalb Deutschlands zu adressieren, beispielsweise falls keine Korrespondenz-Bankbeziehungen existieren. Zusätzlich sind grenzüberschreitende Zahlungen in Drittwährungen möglich. Erreichbar sind direkt ungefähr 3.500 Niederlassungen.

Der ELS verrechnet Zahlungen im Echtzeit-Bruttoverfahren. Er ist speziell für eilbedürftige Zahlungsaufträge und Großzahlungen entworfen. Das ELS arbeitet bei der Zahlungsabwicklung nach dem Deckungsprinzip, wobei die Banken zinslose Innertageskredite bei der Deutschen Bundesbank in Anspruch nehmen können. Diese sind über hinterlegte Pfänder bei der Bundesbank gesichert.

Banken können über ihr Zentralbankkonto an dem ELS teilnehmen, andere Institutionen beispielsweise private Unternehmen gehen über die kontoführende Stelle der Bundesbank. Ausländische Institute ohne Präsenz in Deutschland können via SWIFT und Fernzugang[145] an den ELS angebunden werden. Indirekt können Institute ohne Bundesbankkonto über ein bereits angeschlossenes Institut am ELS teilnehmen.

Die Übermittlung der Zahlungsdaten zwischen den Teilnehmern und dem ELS erfolgt in der Regel per Datenfernübertragung (DFÜ) oder per Datenträger, in Einzelfällen ist eine beleghafte Einreichung möglich. Die Teilnehmer müssen aufgrund der Bruttoverrechnung keine besonderen Bonitätsüberprüfungen durchlaufen, lediglich die technische Infrastruktur muss zur Verfügung stehen.

4.2.2.1.3 Elektronische Abrechnung Frankfurt

Die Elektronische Abrechnung Frankfurt (Euro Access Frankfurt (EAF)) war ein vollelektronisches Clearing-Verfahren der Landeszentralbank Hessen und verband Ansätze von Brutto- und Nettoverfahren (Hybrid-System). Aus diesem Grund wird das System stellvertretend für ähnlich aufgebaute Systeme anderer Länder an dieser Stelle kurz skizziert.

In der EAF wurden Zahlungen teilnehmender Banken bilateral oder multilateral verrechnet (minimiert Liquiditätseinsatz, entspricht Nettoverfahren). Grenzüberschreitende Zahlungen konnten direkt zwischen Teilnehmern verrechnet werden. Die EAF diente der gleichtägigen Verrechnung und Abwicklung von Zahlungen aus dem Geld- und Devisenhandel, von Inlandskundenzahlungen sowie von kommerziellen Zahlungen aus dem Korrespondenzbankengeschäft. Das tagesdurchschnittliche Abwicklungsvolumen lag bei ca. 150 Mrd. Euro oder 50.000 Zahlungen und war seinerzeit das höchste aller Euro-Zahlungssysteme.[146]

Die Zahlungsnachrichten wurden in Form von Zahlungsaustauschdateien per Datenfernübertragung (DFÜ) an das EAF-System geschickt. Nach der Verrechnung wurden diese Daten ebenfalls per DFÜ an die Empfängerbank weitergeleitet. Der Austausch der Zahlungsnachrichten zwischen EAF und den Fernzugangs-Teilnehmern erfolgte über den FIN-Service von SWIFT (zu SWIFT vgl. ausführlich 4.2.4.). Um den EAF-Betrieb vor missbräuchlichem Zugriff abzusichern und zum Schutz vor Manipulationen an den Dateien, wurden die Zahlungsdaten verschlüsselt. Die EAF verfügte über ein umfangreiches Backup-Verfahren zur Datensicherung (alle Systeme waren doppelt ausgelegt) und konnte Zahlungsdaten auch

[145] Ausländische Finanzinstitute können unter bestimmten Voraussetzungen per Fernzugang, d.h. ein Institut muss keine inländische Filiale nachweisen, die nationalen Individual-Zahlungssysteme nutzen (EU-Diskriminierungsverbot).
[146] Vgl. LZB (1999), S. 8.

über Datenträger annehmen oder ausliefern. Die technische Verfügbarkeit der EAF lag im Jahresdurchschnitt bei über 99,9%.[147]
Mittels speziellen Informationsformaten konnten die Teilnehmer jederzeit ihren Finanzstatus in der EAF bestimmen. Weitere Nachrichtendateien dienten zur Versendung allgemeiner Systeminformationen für die Teilnehmer. Die Teilnehmer konnten über solche Dateien beispielsweise Optionen für die Zahlungsausführung festlegen und Order für Liquiditätsoperationen erteilen. Diese Dienste finden sich erweitert auch im heutigen RTGS^{plus} wieder.

4.2.2.1.4 Großbetrag-Scheckeinzug

Schecks, die Beträge von € 3.000 überschreiten, und die auf Kreditinstitute im Inland gezogen sind, werden von der Bundesbank im Rahmen des Großbetrag-Scheckeinzugs (GSE) in Datensätze umgewandelt. Der Gegenwert wird über das EMZ-Verfahren[148] beleglos eingezogen.[149] Die Schecks in Papierform werden zu Kontrollzwecken den entsprechenden Kreditinstituten zugestellt. In den letzten Jahren versucht die Deutsche Bundesbank durch die Preisgestaltung, die zuletzt am 01.07.2002 stark zugunsten standardisierter elektronischer Übertragungswege geändert wurde, Einfluss auf die Marktteilnehmer zu nehmen und elektronische Wege zu bevorzugen. Diese Gestaltungsmöglichkeit hat die Bundesbank wegen ihrer Monopolstellung im Bereich der Umwandlung von Schecks bewusst genutzt.[150]

Die Deutsche Bundesbank hat im Jahr 2001 im GSE-Verfahren circa 142.000 Einzugspapiere mit einem Gesamtvolumen von € 3,4 Mrd. bearbeitet.[151]

4.2.2.1.5 Auslandszahlungsverkehr

Über den Auslandszahlungsverkehr (AZV) werden Überweisungen ins oder aus dem Ausland abgewickelt.[152] Das AZV-Verfahren ist im Gegensatz zu TARGET für Zahlungen in jeder Währung in Länder auch außerhalb der Euro-Zone geeignet. Technische Grundlage für Überweisungen ins Ausland sind die Systeme RTGS^{plus} und bis 2004 der Elektronische Schalter.

Die Abwicklung der Zahlungen mit dem Ausland erfolgt nach dem Korrespondenzbankprinzip. Die Bundesbank unterhält im Ausland bei ausländischen Korrespondenten Konten in der jeweiligen Landeswährung (Nostrokonten). Die Bundesbank ihrerseits führt für ausländische Banken Lorokonten, die auch einen Fernzugang der Institute zum TARGET-System[153] ermöglichen. Zahlungen aus dem Ausland laufen als SWIFT-Inlandsanschlusszahlungen über RTGS^{plus} oder ELS an die jeweiligen Finanzinstitute, sofern sie nicht auf Korrespondenzkonten verrechnet werden können.

Die Überweisungen können sowohl beleglos als auch beleghaft bei der Bundesbank eingereicht werden. Die Weiterleitung erfolgt über SWIFT.

---

[147] Vgl. LZB (1999), S. 14.
[148] Siehe 4.2.2.2.1.
[149] Vgl. Deutsche Bundesbank (2003f).
[150] Vgl. Friederich (2001), S. 5 f.
[151] Deutsche Bundesbank (2002c), S. 9.
[152] Vgl. Deutsche Bundesbank (2003f).
[153] Siehe 4.2.3.3.

4.2.2.2 Angebot der Deutschen Bundesbank im Massenzahlungsverkehr

Im Bereich des Massenzahlungsverkehrs ist die Deutsche Bundesbank nicht so „marktbeherrschend“ wie bei den Großzahlungen. Sie bietet dennoch eine breite Palette von Dienstleistungen an:

- Elektronischer Massenzahlungsverkehr (EMZ) mit Überweisungen und Lastschriftverfahren
- Belegloser Scheckeinzug (BSE)
- Beteiligung der Bundesbank an STEP2 der European Banking Association (EBA).[154]

4.2.2.2.1 Elektronischer Massenzahlungsverkehr

Mit dem Verfahren „Elektronischer Massenzahlungsverkehr“ (EMZ) wickelt die Deutsche Bundesbank Massenzahlungen im Bereich Überweisungen und Lastschriften ab.[155] Beim Massenzahlungsverkehr besteht in der Regel keine oder zumindest eine niedrigere Priorität für einzelne Zahlungen als bei Großbetragszahlungen. Als Massenzahlungen gelten Überweisungsaufträge (sogenannte Prior3-Zahlungen), Lastschrift- und Scheckeinzüge, die mit eintägiger Laufzeit von der Bundesbank bearbeitet werden. Der EMZ-Überweisungsverkehr wird seit 5.2.1999 floatfrei abgewickelt, das heißt Belastung und Gutschrift auf den jeweiligen Konten erfolgen taggleich am Tag nach der Einreichung, ein beim Einzugsverkehr vorher bereits gültiges Prinzip. Im Durchschnitt wurden 2001 pro Arbeitstag 9 Mio. Aufträge im EMZ bearbeitet, in der Spitze bis zu 25 Mio. Dabei sind ca. ein Drittel der Aufträge Überweisungen, die anderen zwei Drittel Lastschriften (ca. 40 %) und Scheckgegenwerte.[156]

Gegen mögliche Insolvenzen der Teilnehmer am EMZ-Verfahren sichert sich die Deutsche Bundesbank mit Sperrmechanismen ab, die eine Glattstellung der Konten erst bei Deckung auf dem jeweiligen Konto (oder vorhandenen Sicherheiten) ermöglichen.

Die Zahlungsdaten werden im DTA-Format beleglos auf Datenträgern bei den Filialen der Bundesbank oder deren Rechenzentrum eingereicht. Die Verarbeitung der Zahlungsdaten erfolgt in den Abendstunden des Eingangstages; die Banken erhalten diese Daten am nächsten Morgen auf Datenträgern/per DFÜ. Seit der Vorbereitungsphase auf die europäische Währungsunion ist der Markt für Zahlungssysteme generell stärker in Bewegung geraten. Im Umfeld des zunehmenden Wettbewerbs wurde und wird auch der EMZ stufenweise modernisiert.[157] So ist seit März 2000 die Datenübertragung per DFÜ möglich (seit 2002 mit dem im Kreditgewerbe verwendeten OFTP-Standard), so dass Zahlungsdaten bis abends direkt beim Rechenzentrum angeliefert werden können. Nach dem Verrechnungslauf erfolgt die Auslieferung an die Banken per DFÜ. Gegenwärtig wird an weiteren Datenformaten gearbeitet, unter anderem soll geklärt werden, ob die SWIFT-Nachrichtenformate eine geeignete Basis für den EMZ darstellen könnten. Die Diskussion um den Einsatz modernerer Sicherungsverfahren und den Einsatz internationaler Nachrichtenformate im nationalen Zahlungsverkehr läuft bereits seit einigen Jahren.[158]

[154] Vgl. 4.2.3.5.4.
[155] Vgl. Deutsche Bundesbank (2003f).
[156] Deutsche Bundesbank (2002), S. 3.
[157] Vgl. Friederich (2001), S. 2 ff., Deutsche Bundesbank (2002c).
[158] Vgl. Fabritius (2001), S. 14, Deutsche Bundesbank (2002).

4.2.2.2.2 Belegloser Scheckeinzug

Seit 7.9.1998 müssen Kreditinstitute gemäß im ZKA verhandelten Abkommen für den Einzug von (Reise)-Schecks (Scheckabkommen/Reisescheckabkommen) die Daten von Schecks unter € 3.000 elektronisch erfassen und über das beleglose Scheckeinzugsverfahren abwickeln. Dies gilt aber nur für auf Kreditinstitute im Inland gezogene Schecks, und wenn alle fünf Felder der Codierzeile korrekt gelesen wurden. Zusätzlich gibt es die Möglichkeit über ein Prüfzifferberechnungsverfahren die richtige Erfassung der Kontonummer zu überprüfen. Die Belege der elektronisch erfassten Schecks bleiben im umwandelnden Rechenzentrum (im Gegensatz zu Schecks, die auf höhere Beträge ausgestellt sind). Wegen Umwandlungsproblemen nicht BSE-fähige Schecks gehen ins GSE-Verfahren[159] über. Sind die Schecks in beleglose Zahlungen umgewandelt, erfolgt der Einzug der Scheckgegenwerte im EMZ-Verfahren[160].

4.2.3 Supranationale Zahlungsverkehrsnetze und -verfahren: Massen- und Großzahlungssysteme

4.2.3.1 Zahlungsverrechnung im Euro-Währungsraum

Die Zahlungsströme im Euro-Währungsraum nehmen zu. Die ökonomische und politische Entwicklung zur Single European Payment Area hat die Systementwicklung wesentlich beeinflusst. Eine Zahlung kann innerhalb des Euro-Währungsraumes vielfältige Wege nehmen. Die bedeutendsten werden in Abbildung 9 dargestellt.

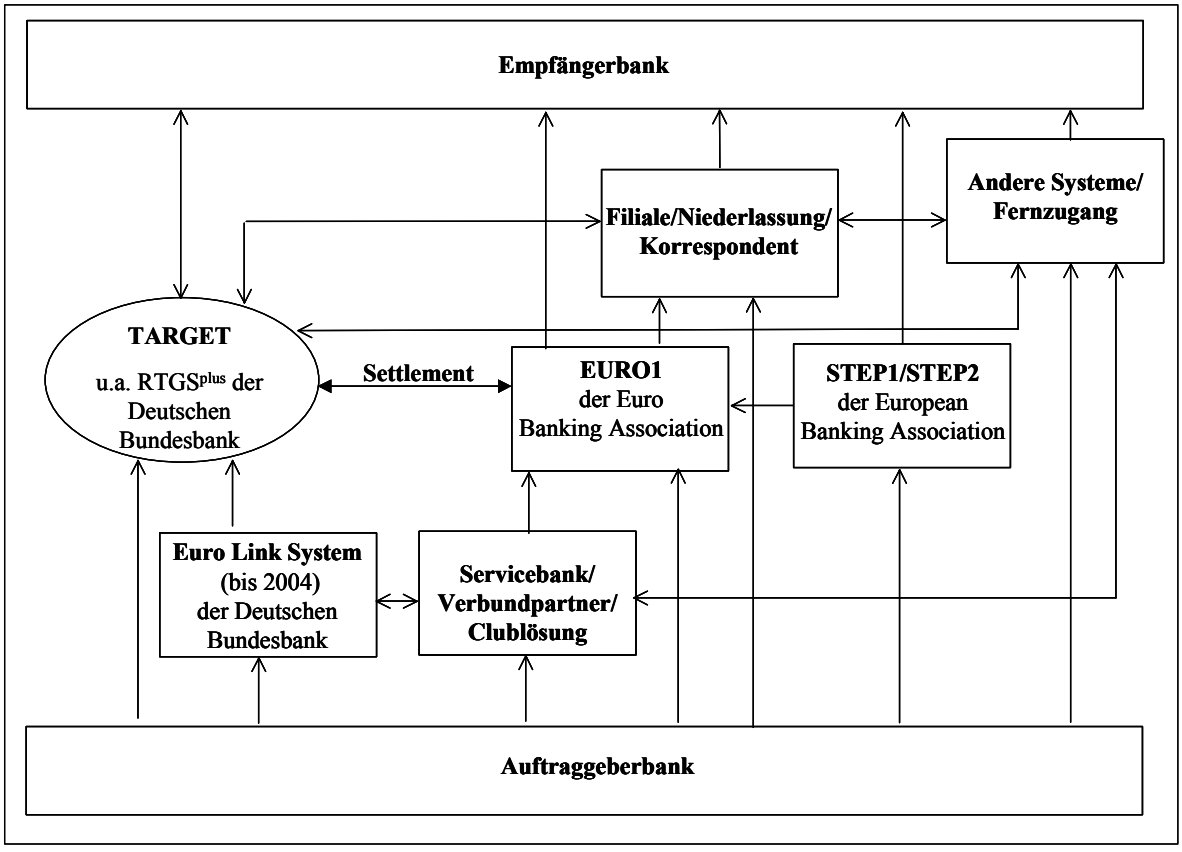

Abbildung 9: Wege der Zahlungsverrechnung im Euro-Währungsraum[161]

[159] Siehe 4.2.2.1.4.
[160] Siehe 4.2.2.2.1. Vgl. Deutsche Bundesbank (2003f).
[161] Eigene Darstellung/Aktualisierung, in Anlehnung an Friederich (2000), S.2.

Die Trennung zwischen Großzahlungs- und Massenzahlungsverkehr wird auf europäischer Ebene zwar nicht aufgehoben, gleichwohl nähern sich die Abwicklungsverfahren technisch an. So stellt sich das Zahlungsverfahren STEP1 für die Abwicklung von Kundenzahlungen auch im niedrigen Segment letztlich als Zugangsmöglichkeit zum EURO1-System dar, für Banken, die die hohen Anforderungen an die direkte Teilnahme an EURO1 nicht erfüllen können oder wollen.

Ein wesentlicher Weg (vorbei an den bekannten Großzahlungssystemen), über den europäische wie internationale Zahlungen verrechnet werden, ist die Zahlungsverrechnung über Korrespondenzbanken.

4.2.3.2 Zahlungsverkehr über Korrespondenzbanken

Korrespondenzbankbeziehungen und -dienste werden sowohl national als auch international für den Zahlungsverkehr genutzt. Grundsätzliches Prinzip einer Korrespondenzbankbeziehung ist eine vertragliche bilaterale Vereinbarung, auf deren Basis ein Finanzinstitut für ein anderes (Zahlungsverkehrs-)Dienstleistungen erbringt. Technisch wird diese Dienstleistung durch gegenseitige Konten ermöglicht, so genannte Loro- und Nostrokonten[162], die vorgegebene Kreditlinien beinhalten können. Es existiert ein weltweites Netz von Korrespondenzbank-Beziehungen, mit dem Teile des grenzüberschreitenden Zahlungsverkehrs ohne die etablierten Großzahlungs-Systeme abgewickelt werden können.

Es kann die Zahlungsverkehrsabwicklung über die direkte Kontoverbindung, über Agenturvereinbarungen und über Auslandstöchter unterschieden werden. Die Unterhaltung direkter Kontoverbindungen ist bei geringen Volumina kostenintensiv, so dass sich Clublösungen etabliert haben, die einen gemeinsamen „entry point“ in das weitere Zahlungsnetz haben, und somit eine geringere Anzahl an Loro-/Nostro-Konten und teuren Abstimmungsprozeduren benötigen.[163]

Die Verwendung von bestimmten Datenformaten im Korrespondenzbanken-Verkehr ist Gegenstand bilateraler Vereinbarungen, in der Regel wird SWIFT als Kommunikationsplattform genutzt.

Die Bedeutung der Korrespondenzbankbeziehungen für den Auslandszahlungsverkehr ist erheblich. Der Bundesverband deutscher Banken geht davon aus, dass die Abwicklung des grenzüberschreitenden Euro-Zahlungsverkehrs innerhalb der EU zu mehr als 50 % über kontenbasierte Korrespondenzbankbeziehungen abgewickelt wird.[164] Die jährlichen Zuwachsraten der Individual-Zahlungssysteme seit 2000 von ca. 15 % pro Jahr im Euro-Raum deuten allerdings darauf hin, dass Korrespondenzbank-Beziehungen weniger benutzt werden.[165]

Die Effizienz, Qualität und auch Sicherheit von Zahlungen über diese Beziehungen ist im Vergleich zu den standardisierten Verfahren, die bei EURO1 und TARGET zur Geltung kommen, äußerst zweifelhaft.[166] Gleichwohl ist erst durch die EU-Kommission und deren Preis- und Zeitvorgaben innerhalb des europäischen Zahlungsverkehrs sowie die ambitionierten Ziele der Single European Payment Area (SEPA) Bewegung in dieses etablierte System

[162] Lorokonto: Von Korrespondenzbank im Auftrag einer ausländischen Bank geführtes Konto. Nostrokonto: ein im Ausland bei einer Korrespondenzbank für die eigene Bank geführtes Konto.
[163] Vgl. Rehm (2001), S. 15 f.
[164] Vgl. BdB (2003b), S. 19.
[165] Vgl. Deutsche Bundesbank (2002), S. 61.
[166] Vgl. Ullrich (2001), S. 2, BdB (2003b), S. 19, Riedl (2002), S. 43.

gekommen. Rehm gibt offen zu, dass die Banken noch in den neunziger Jahren das Korrespondenzbankprinzip so stark eingeschätzt haben, dass die Entwicklung effizienterer Verfahren nicht realisiert wurde. Er kommt zu dem Schluss:[167] „Angesichts des zu erwartenden Preisdiktats der EU-Kommission hat das Correspondent-Banking im Euro-Raum keinerlei Zukunft."

4.2.3.3 TARGET

Die Einrichtung eines Interbank-Überweisungssystems der Zentralbanken der Europäischen Union „Trans-European Automated Real-time Gross Settlement Express Transfer" (TARGET) ist vom Rat des Europäischen Währungsinstituts formal für den Start der 3. Stufe der Europäischen Wirtschafts- und Währungsunion beschlossen worden. TARGET ist ein dezentral konzipiertes europäisches Zahlungssystem und wird seit dem 4.1.1999 eingesetzt. Es ist ein transaktionsorientiert in Echtzeit arbeitendes Verfahren, das die 15 nationalen Echtzeit-Bruttozahlungssysteme der europäischen Zentralbanken (RTGS^{plus} und ELS in Deutschland) und das Zahlungsverkehrssystem der EZB, der European Payment Mechanism (EPM), europaweit verbindet. Die Verbindung wird technisch über das so genannte Interlinking-System ermöglicht, ein Echtzeit-Kommunikationsnetz auf SWIFT-Basis. Das Interlinking-System ist einerseits ein IT-System zur Verwaltung der TARGET-Verrechnungskonten zwischen den nationalen Zentralbanken und andererseits ein Telekommunikationsnetzwerk, das die relevanten Daten in Echtzeit übermittelt.[168]

TARGET ist das erfolgreichste Großzahlungssystem in der Europäischen Union und hat 2002 wertmäßig 85 % aller europäischen Großzahlungen abgewickelt (59 % der Transaktionen).[169] Es wird sowohl zur Abwicklung geldpolitischer Operationen durch die EZB genutzt, als auch von der EBA Clearing Organisation für die Verrechnung bei den Zahlungssystemen EURO1 und teilweise STEP2 verwendet, sowie vom Devisenabwicklungssystem CLS (Continious Linked Settlement) zum Verrechnen der Tagesendstände. Es besteht keine Betragsbegrenzung für die an TARGET angeschlossenen Banken, so dass theoretisch alle Zahlungen über TARGET abgewickelt werden könnten. Während TARGET als Interbanken-Zahlungssystem in Europa keine Konkurrenz hat, gibt es für Kundenzahlungen Alternativen, beispielsweise die Korrespondenzbankbeziehungen oder EURO1. Gleichwohl steigt der Anteil der Kundenzahlungen am gesamten Zahlungsaufkommen kontinuierlich und erreichte 2002 bereits 45,5 % der Transaktionszahlen.[170]

Eine Bank, die TARGET einsetzen will, muss zunächst an das nationale Real-Time Gross Settlement System (RTGS) angeschlossen sein, oder über einen entsprechenden Fernzugang bei einer anderen europäischen Zentralbank verfügen. Die verwendeten Nachrichtenformate sind die für den Zahlungsverkehr üblichen SWIFT-Formate MT 100 (wird ab November 2003 durch MT 103 ersetzt), MT 103 (Kundenzahlungen mit STP-Eigenschaften) und MT 202 (Interbankenzahlungen mit STP-Charakteristik). Im Interlinking-System wird MT 198 eingesetzt, um die Konvertierung nationaler Datensätze in die für das Empfängerland passende Form zu ermöglichen.[171]

Jede Zahlung wird in TARGET individuell abgearbeitet, parallel zur Ausführung der Zahlung wird in Echtzeit (faktisch Sekunden bis Minuten) die jeweilige Zentralbank benachrichtigt.

[167] Rehm (2001), S. 15.
[168] EZB (2000e), S. 13.
[169] EZB (2003c), S. 6.
[170] EZB (2003c), S. 7.
[171] Vgl. BdB (2003b), S. 33. Zu SWIFT im Detail siehe 4.2.4.

Die Zahlungen werden in Zentralbankgeld getätigt und sofort final dem Konto des Begünstigten gutgeschrieben. Damit entfällt insbesondere das immanente Verrechnungsrisiko reiner Nettosysteme. Ein wesentlicher Erfolgsfaktor von TARGET ist die hohe verfügbare Liquidität im System, unter anderem ist es Geschäftsbanken möglich, auf taggleich zinsfreie Zentralbankkredite zuzugreifen.[172]

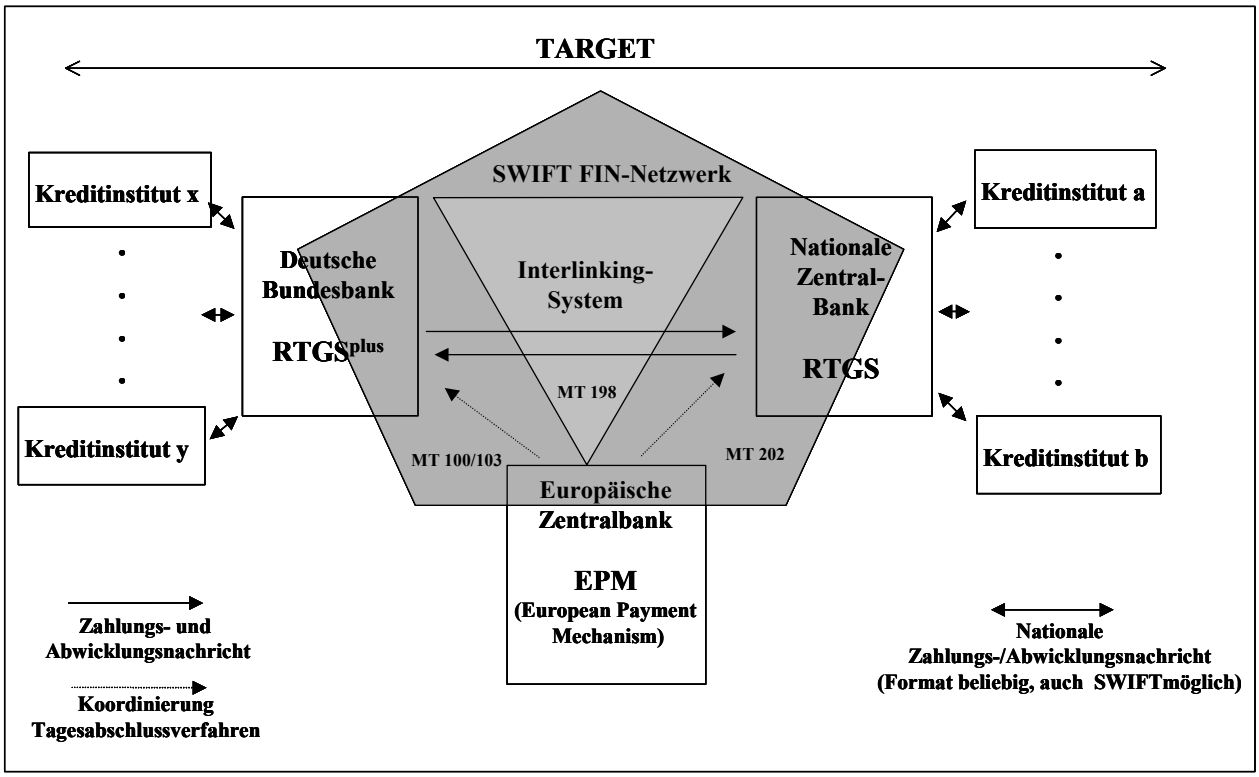

Abbildung 10: Aufbau von TARGET und Nachrichtenfluss in TARGET

In Abbildung 10 wird der Aufbau und die Funktionsweise von TARGET schematisch am Beispiel von Interbankenzahlungen über die deutsche RTGS^{plus}-Komponente von TARGET zu einem nationalen RTGS-System einer beliebigen anderen europäischen Zentralbank dargestellt. Das auftraggebende Kreditinstitut leitet den TARGET-Zahlungsauftrag je nach nationaler Anbindung an RTGS^{plus}. Dort wird die Gültigkeit des Auftrags überprüft und sichergestellt, dass kein vorgegebenes Limit überschritten wird. Ist der Auftrag legitimiert, und die empfangende nationale Zentralbank (NZB) betriebsbereit, wird der Überweisungsbetrag unwiderruflich dem Zentralbankkonto der auftraggebenden Bank belastet, und auf dem Interlinking-Verrechnungskonto der empfangenden NZB bei der Deutschen Bundesbank gutgeschrieben. Die Zahlungsnachricht wird über das Interlinking-Netzwerk an die empfangende NZB geleitet. Der Datenaustausch zwischen den nationalen Interlinking-Komponenten der Zentralbanken basiert auf einer von SWIFT zur Verfügung gestellten Infrastruktur zur Nachrichtenübermittlung, dem SWIFT FIN Network. Die ausländische NZB überprüft ebenso wie zuvor die Deutsche Bundesbank die Syntax des Datensatzes und stellt fest, ob die begünstigte Bank am nationalen RTGS-System teilnimmt, und das RTGS-System überhaupt erreichbar ist. Im negativen Fall werden entsprechende SWIFT-Fehlermeldungsformate genutzt. Bei positiver Prüfung wird das Interlinking-Konto der Deutschen Bundesbank bei der ausländischen NZB belastet. Die erhaltene Zahlungsnachricht wird je nach Erfordernis durch das Interlinking System in TARGET in das Datenformat des nationalen Bruttosystems

[172] Vgl. EZB (2003e), S. 2.

umgewandelt und an die Empfängerbank weitergeleitet. Die Gutschrift erfolgt auf dem Konto der Empfängerbank bei der NZB. Die Abwicklung des Auftrages wird mit einer Quittungsmeldung über das nationale RTGS-System an die Deutsche Bundesbank bestätigt. Der gesamte Zahlungsvorgang geschieht in Echtzeit, de facto in Sekunden bis maximal Minuten. Fehlt die Quittung nach 30 Minuten immer noch, wird individuell ermittelt.

Die EZB selbst ist an der Zahlungsabwicklung nicht beteiligt. Erst am Ende eines Geschäftstages stellt die EZB in einem Abstimmungsverfahren sicher, dass alle Transaktionen fehlerfrei abgeschlossen wurden. Der Zahlungsausgleich unter den nationalen Zentralbanken erfolgt anschließend über die Konten, welche diese bei der EZB unterhalten.

TARGET hat 1560 direkte Teilnehmer, indirekt können über 40.000 Kreditinstitute angesprochen werden, das bedeutet fast alle Kreditinstitute innerhalb der EU haben einen Zugang zu TARGET.[173] TARGET wird nicht nur für Interbankengeschäfte eingesetzt, zunehmend führen Unternehmen grenzüberschreitende Zahlungen mit TARGET durch. Waren es 2000 noch 30 % der gesamten über TARGET grenzüberschreitend abgewickelten Zahlungen, hat sich deren Anteil in TARGET 2002 auf über 45 % erhöht. Mit der Folge, dass 77 % aller Zahlungen unter € 50.000 lagen. 2002 wurden 64,5 Millionen Zahlungsaufträge in TARGET bearbeitet – arbeitstäglich im Schnitt 253016 Zahlungen – mit einem Gegenwert von € 395 Billiarden.[174] Fast 80 % der Zahlungen (in Stück) sind jedoch nationale Zahlungen, die über die inländischen RTGS-Komponenten von TARGET abgewickelt werden. Sie machen wertmäßig jedoch „lediglich“ 54,5 % der Zahlungen in TARGET aus. TARGET ist das weltweit größte Zahlungssystem;[175] allerdings handelt es sich zumindest bei der jetzigen TARGET-Version durch den dezentralen Aufbau um einen Zahlungssystem-Verbund.

Die Verteilung der Zahlungsströme innerhalb von TARGET ist äußerst heterogen. Vier Systeme (Deutschland, Italien, Frankreich und die Niederlande) wickeln rund 77 % aller Zahlungen ab.[176] Eine Express-Zahlung verblieb im September 2002 durchschnittlich 1.02 Minuten im TARGET-Netz, die Verfügbarkeit des Kern-Systems lag seit Betriebsbeginn bei nahezu 100%, 99,75 % im Jahr 2001 und 99,77 % im Jahr 2002.[177] Im Jahresbericht wurden für 2002 lediglich 6 größere Zwischenfälle gemeldet[178], einmal mit der Verbindung EPM und SWIFT, die anderen Male waren nationale RTGS-Systeme ausgefallen – am längsten beeinträchtigte für 7 Stunden ein Softwarefehler die Bank of England, ein Streik führte für drei Tage zu Problemen im griechischen System. In allen Fällen konnten die systemkritischen Großzahlungen trotzdem taggleich bearbeitet werden. Im Eurosystem werden seit 2002 neben systemkritischen (critical) Zahlungen (Geldpolitische Operationen, Tagesendverrechnung in EURO1 etc.) zusätzlich noch sehr kritische (very critical) Großzahlungen unterschieden. Letztere sind alle Zahlungen, die mit CLS in Verbindung stehen.

Die TARGET-Systembetreiber führen regelmäßig Risikoanalysen durch, die neben der IT-Infrastruktur, die Software, die Prozesse und die Notfallpläne umfassen. Als technische Sicherheitsziele, die in TARGET erfüllt sein sollen, werden die Sicherstellung der Systemintegrität sowie die Verfügbarkeit, Vertraulichkeit, Authentizität und Nichtabstreitbarkeit der Daten genannt – weitere Dokumente zur Sicherheitsstruktur sind vertraulich. Bisher sind

[173] EZB (2003e), S. 4.
[174] 2002 war TARGET an 255 Tagen erreichbar.
[175] EZB (2003e), S. 4, EZB (2003c), S. 6.
[176] BdB (2003b), S. 36.
[177] EZB (2003e), S. 3. Als Verfügbarkeit gilt die durchschnittliche Verfügbarkeit der an TARGET teilnehmenden RTGS-Systeme.
[178] EZB (2003c), S. 19 f.

diese Maßnahmen erfolgreich, es sind weder Betrugsfälle noch größere Ausfallzeiten öffentlich geworden. Die hohe Verfügbarkeit wird unter anderem durch redundante Systeme (Back-up-Rechner) erreicht, die in kürzester Zeit (maximal 4 Stunden) erreichbar sein müssen, falls das primäre System ausfällt (wiederum dezentral geregelt). Das TARGET Informations System (TIS), implementiert im Oktober 2000, versorgt die Teilnehmer zeitnah über die gängigen Informationsdienste Reuters, Telerate/Bridge und Bloomberg mit systemrelevanten Informationen insbesondere bei Störungen, so dass diese sich auf die veränderten Umstände einstellen können.[179] Von Bedeutung ist insbesondere die Meldung über den Ausfall nationaler RTGS-Systeme, damit für dringende Zahlungen alternative Wege, beispielsweise Korrespondenzbanknetze genutzt werden können.

Die Kreditinstitute regeln den notwendigen Schlüsselaustausch für symmetrische Verschlüsselungsverfahren mit der zuständigen nationalen Zentralbank (oder bei Fernzugängen mit der dortigen Zentralbank) im Rahmen der nationalen RTGS-Systeme. Die Sicherheit des nationalen RTGS-Systems wird national gewährleistet. Der mögliche Ausfall der für TARGET bedeutenden SWIFT-Dienste wird in keinem Sicherheits-/Risikoszenario betrachtet, sondern als Restrisiko akzeptiert.[180]

Die systemische Überwachung von TARGET durch die europäischen Zentralbanken wurde erst im Januar 2003 institutionell festgelegt.[181] Demnach sind die nationalen Zentralbanken für die Sicherheit ihres jeweiligen RTGS-Systems und die EZB für den European Payment Mechanism in TARGET zuständig. Die koordinierenden Tätigkeiten für die nationale Überwachungsarbeit liegen bei der Payment Systems Policy Working Group (PSPWG), einer Arbeitsgruppe des Systems der Europäischen Zentralbanken (ESZB), die unabhängig von der TARGET Management Working Group (TMWG) arbeitet. Die Ergebnisse der Arbeitsgruppen werden dem Payment and Settlement Systems Committee (PSSC) übermittelt, das wiederum dem EZB-Rat untersteht. Ziel ist es, in TARGET vollständig kompatibel mit den von der BIZ erarbeiteten „Core Principles for Systemically Important Payment Systems“[182] zu sein. Im Rahmen dieser Arbeiten wird auch das Risikomanagement der nationalen Systembetreiber auf den Prüfstand gestellt und überarbeitet.

4.2.3.4 Weiterentwicklung TARGET2

Der Erfolg von TARGET ist nicht zwingend auf seine dezentrale Konzeption zurückzuführen, vielmehr auf die Monopolstellung und die (für die Euroeinführung notwendige) schnelle Umsetzung des Verfahrens, die erst durch den Rückgriff auf die dezentral bereits verfügbaren RTGS-Systeme möglich wurde. Gleichwohl gibt es verschiedene Gründe, die eine Weiterentwicklung dieses Systems zwingend erforderlich machen:[183]

- Im Extremfall müssten nach der Erweiterung der Europäischen Union 25 einzelne RTGS-Systeme in TARGET koordiniert werden,
- TARGET ist in Bezug auf die Leistungsstruktur heterogen, einzelne RTGS-Komponenten sind deutlich performanter als andere,
- Kosteneffizienz ist durch das dezentrale Konzept schwer zu erreichen,
- die Notfallpläne sind uneinheitlich,
- die Preisstrukturen in TARGET sind nicht homogen,

[179] Vgl. EZB (2003c), S. 20.
[180] Vgl. Münch (2002), S. 132 ff.
[181] Vgl EZB (2003c), S. 26f.
[182] Vgl. BIZ (2001b eng.) und 5.1.3.1.2.
[183] Vgl. BdB (2003b), S. 33 f. und EZB (2003c), S. 28f.

- die dezentrale Struktur erfordert teure Harmonisierungsanstrengungen und verhindert einheitliche Service-Levels,
- die Belange der Nutzer von TARGET sind bislang nicht hinreichend berücksichtigt, z. B. eine zentrale Liquiditätssteuerung oder Real-Time-Informationen für die Nutzer über ihre Euro-Positionen.

Die Fortentwicklung von TARGET zu TARGET2, von der EZB koordiniert,[184] ist neben der Frage technischer Details und der Festlegung einheitlicher Dienstleistungen und der bereits jetzt ungleichen Verteilung der Last der Zahlungsaufträge auf die einzelnen Systemkomponenten eine politische Frage.[185] Wer betreibt ein harmonisiertes System? Kann eine einzelne nationale Zentralbank, oder können die 5 größten RTGS-Systembetreiber die anderen Betreiber aus dem Markt drängen? Es geht bei der Antwort auf diese Fragen um Einflussnahme, Macht und bei kosteneffizientem Betrieb neben Arbeitsplätzen und Know-How möglicherweise um Gewinne aus dem Betrieb eines Zahlungssystems.

Aus technischer Sicht ist jede Vereinheitlichung insbesondere für Fragen des Krisenmanagements und der Notfallplanung ein Gewinn. In der Folge obiger Überlegungen bleibt TARGET2, wie es im Beschluss des EZB-Rates konzipiert wurde[186], jedoch aus den politischen Gründen heraus zunächst ein Kompromiß und gibt einem„multiplen Plattform-System“[187] den Vorzug. Die Aufgabe, ein harmonisiertes System zu konstruieren, wird als aufwändig eingestuft. Es müssen drei Phasen, Projektvorbereitungs-, Projekt- und Testphase durchlaufen werden. In die Projektvorbereitungsphase fällt die öffentliche Konsultation, bei der den Marktteilnehmern die Möglichkeit gegeben wird, ihre Anforderungen zu spezifizieren. Die EZB rechnet nicht vor „der zweiten Hälfte dieses Jahrzehnts“ mit dem operativen Betrieb von TARGET2.[188] Das Leistungsspektrum soll sich auch in TARGET2 vor allem auf systemkritische Großzahlungen konzentrieren, die EZB betont jedoch, dass analog zu TARGET „there will not be any de jure or de facto limits, set by the Eurosystem or the NCBs, on any payments that users may wish to process in real time in central bank money.“[189] Angesichts der de facto sinkenden Durchschnittshöhe der Zahlungen in TARGET, bedingt durch die zunehmende Anzahl Kundenzahlungen, wäre eine Einschränkung der Betragshöhen auch betriebswirtschaftlich mit Blick auf Skaleneffekte kaum wünschenswert. Der Wettbewerb insbesondere mit EURO1 wird zeigen, welches System für Zahlungen unter € 50.000 im Markt auf Dauer performanter sein wird.

Die Leitungsstruktur für die Entwicklung und den Betrieb von TARGET2 liegt bereits fest.[190] Auf oberster Ebene ist der EZB-Rat angesiedelt, darunter die nationalen Zentralbanken, die an der gemeinsamen Plattform teilnehmen und auf der untersten Ebene die technischen Betreiber, die im Fall der Deutschen Bundesbank mit RTGS^{plus} mit der Zentralbank identisch sind. Beratend begleitet werden alle Ebenen von den Anwendern, die im Rahmen von Konsultationen und Gesprächen an der Ausgestaltung, insbesondere des Leistungsspektrums, von TARGET2 mitwirken können.

Das Konzept sieht vor, nur kosteneffiziente Plattformen auf der TARGET2-Plattform zuzulassen (und letzlich über den Preis eine Vereinheitlichung zu erzwingen). Eine einheitli-

[184] Vgl. EZB (2002f), EZB (2002g).
[185] Vgl. Fabritius (2001), S. 9.
[186] Vgl. EZB (2002f).
[187] EZB (2002g), S. 1.
[188] EZB (2002g), S. 10.
[189] EZB (2002f), S. 1.
[190] EZB (2002g), S. 6f.

che Preisgestaltung für festgelegte Basisdienste wird sowohl für nationale als auch für europäische Eurozahlungen zentral festgelegt. Kerngedanke ist die Entwicklung einer Referenzplattform, die von den NZBen, die dies wünschen und bereit sind, ihr eigenes System aufzugeben, gemeinsam betrieben wird. Erfüllen weitere nationale Systeme die Anforderungen (Preisgestaltung, Leistungsspektrum etc.), die von der Referenzplattform vorgegeben werden, können sie an die gemeinsame Plattform angebunden werden und eigenständig bleiben.[191] Durch ein so genanntes „Active-Active-Konzept" sollen die Aufgaben, das Know-How und das für den Betrieb notwendige Personal für die gemeinsame Plattform auf die beteiligten Länder aufgeteilt werden.

In TARGET2 soll ein Großteil der Leistungen des Zahlungssystems einheitlich europaweit gelten, bei möglicherweise existierenden Unterschieden in der technischen Infrastruktur. Neue Zusatzdienste können erst nach Konsultation der Teilnehmer am System angeboten werden. Als Nachrichtendienst und –format wird auch TARGET2 auf dem SWIFT-Netz aufbauen.[192]

Über die Sicherheitsarchitektur gibt es noch keine öffenlich verfügbaren Dokumente. Die Konsolidierung vieler Plattformen hin zu einer zentralen Plattform werden die sicherheitsrelevanten Prozesse transparenter machen und die Sicherheit aus technischer Sicht erhöhen.

4.2.3.5 Zahlungssysteme der Euro Banking Association

4.2.3.5.1 Euro Banking Association

Die Euro Banking Association (EBA) wurde im Jahr 1985 von 18 europäischen Geschäftsbanken gemeinsam mit der European Investment Bank mit Unterstützung der EU-Kommission und der BIZ gegründet. Heute zählt die EBA mehr als 190 Mitgliedsbanken aus allen Ländern der Europäischen Union. Die EBA ist eine Gesellschaft nach französischem Recht mit Sitz in Paris. Sie diente bis zur Euro-Umstellung zur Förderung des ECU-Zahlungsverkehrs und zum ECU-Clearing. In ihrem Selbstverständnis sieht sich die EBA als Forum der europäischen Zahlungsverkehrsunternehmen, in dem paneuropäische Zahlungsverkehrsinitiativen vorangetrieben werden.[193]

Seit Juni 1998 ist die EBA über die EBA Clearing Company S.A., Paris, Betreiberin verschiedener Zahlungssysteme: zunächst des Großzahlungssystems EURO1 und des Massenzahlungssystems STEP1 und seit 2003 auch des paneuropäischen Massenzahlungssystems STEP2. Die STEP-Zahlungssysteme sind Ergebnis des Programms zur Förderung paneuropäischer Zahlungen S.T.E.P.S. (Straight Through Euro Payment System). STEP1 wurde am 20.11.2000 gestartet und ist im Wesentlichen ein Zugang für Nicht-EURO1-Banken zu EURO1. STEP2 ist ein wesentlicher Schritt hin zu einem paneuropäischen Massenzahlungssystem auf Basis eines Automated Clearing House (ACH).

4.2.3.5.2 EURO1

EURO1 ist ein multilaterales Netto-Clearingsystem und dient seit 04.01.1999 hauptsächlich der Abwicklung grenzüberschreitender Zahlungen im Individualzahlungsverkehr. Als technische Grundlage für die Entwicklung von EURO1 diente die vorher bereits existierende ECU-Clearing Infrastruktur der EBA. Das System arbeitet liquiditätssparend und entspricht

[191] Vgl. EZB (2002g), S. 2.
[192] Vgl. EZB (2002g), S. 4.
[193] www.abe.org.

den Lamfalussy-Kriterien der zwingenden Finalität einer erfolgten Zahlung bei fehlender Rückabwicklungsmöglichkeit.[194]

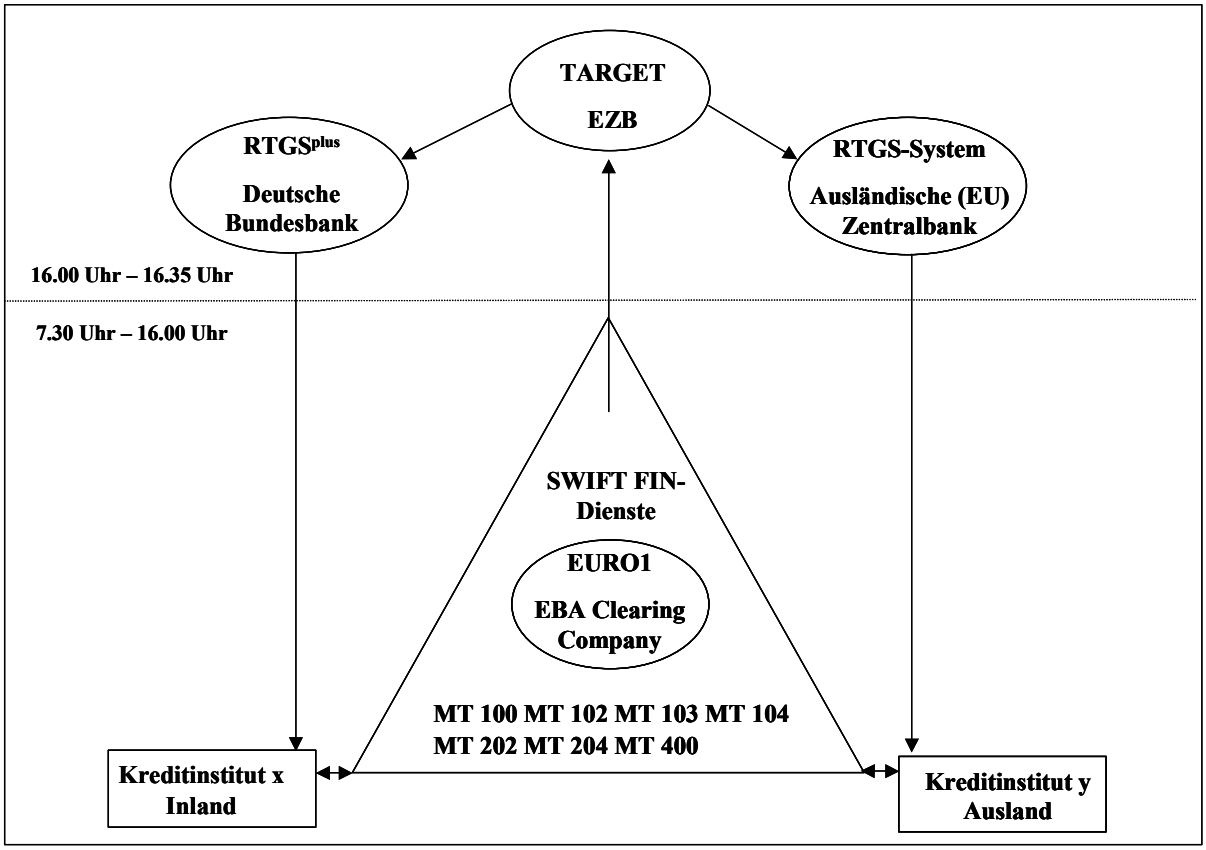

Abbildung 11: Ablauf einer paneuropäische Zahlungsverrechnung in EURO1[195]

74 Kreditinstitute sind an EURO1 als Direktteilnehmer angeschlossen, 38 weitere sind als Tocher-Banken von EURO1-Direktteilnehmern ebenfalls direkt angeschlossen. Sitz der Betreibergesellschaft EBA Clearing Company ist Paris, abgewickelt werden die Zahlungen nach deutschem Recht (Kontokorrentprinzip). Aufsicht über EURO1 führt die EZB, die als „Settlement Agent" auch den Zahlungsausgleich der aufgelaufenen Nettopositionen am Ende eines Tages (16.30 Uhr) per TARGET übernimmt (siehe Abbildung 11).

Der Nachrichtenaustausch erfolgt analog zu TARGET in Form der SWIFT-Nachrichtentypen. Mit den Formaten MT 100, MT 102, MT 103, MT 202 und MT 400 stehen mehr Basisdienste als bei TARGET zu Verfügung. Seit Anfang 2003 werden zusätzlich die Formate MT 104 (Kundenlastschriften/Cash Management) und MT 204 (Gebührenverrechnung, Scheckeinzug und Dokumentengeschäft) unterstützt.

SWIFT bietet als Dienstleister im EURO1-System den Teilnehmern über Terminals weitere Informationen über den Status ihrer Zahlungen, darunter:

- Die aktuelle Höhe bestehender Limits, den Saldo der Zahlungen und der eventuellen Zahlungen in der Warteschlange,
- Details von Zahlungsnachrichten während und zum Ende der Verarbeitungsphase,
- Clearing-Informationen am Ende des Geschäftstages,

[194] Vgl. zu Lamfalussy-Kriterien ausführlich 5.1.3.1.1.
[195] Eigene Darstellung.

- Informationen über Zahlungen einzelner Filialen eines Kreditinstituts zu Reporting-Zwecken und
- Vorabinformationen zu Zahlungen künftiger Valutatage.

In EURO1 läßt sich bezogen auf die durchschnittliche Transaktionshöhe die gleiche Entwicklung feststellen wie in TARGET: Es werden vermehrt niedrigere Beträge abgewickelt. Der Grund ist die zunehmende Ablösung der paneuropäischen Korrespondenzbankzahlungen hin zu EURO1 und TARGET bei Kundenzahlungen, die in der Regel niedriger ausfallen als Innerbankenzahlungen. In EURO1/STEP1, die statistisch zusammen ausgewiesen werden, werden täglich Zahlungen im Wert zwischen 170 und 195 Mrd. € verarbeitet, bei einer durchschnittlichen täglichen Transaktionszahl von ca. 140.000 bis 180.000.[196]

Das Risikomanagement nimmt bei EURO1 eine wichtige Position ein, nicht zuletzt aufgrund der größeren systemischen Unsicherheit von Nettosystemen gegenüber Bruttosystemen wie TARGET. Bei jeder Zahlung wird zunächst der Status der Empfänger- und der Senderbank in Hinblick auf Limits geprüft. Im positiven Fall wird die Nachricht weitergeleitet, im negativen Fall kommt sie in eine Warteschlange. Solange die Zahlung nicht weiter verarbeitet wurde, kann sie vom Sender gestoppt werden. Die rechtliche Grundlage für den Zahlungsverkehr der beteiligten Parteien legt die so genannte „Single Obligation Structure“, die festlegt, dass zu jedem Zeitpunkt nur die Nettoposition jedes Teilnehmers rechtlich bindend verrechnet werden können muss. Anfang 2001 wurde dem EURO1-System vom Internationalen Währungsfond bescheinigt, kompatibel mit den 10 Grundprinzipien für systemisch bedeutsame Zahlungssysteme[197] zu sein.[198]

EURO1 verfügt über weitere systeminterne Merkmale der Risikoverringerung:

- Die Beitrittsbestimmungen für Teilnehmerinstitute sind sehr streng. Unter anderem muss der Hauptsitz des Instituts in einem Land der OECD sein, mit einer Niederlassung in der EU, das Institut muss bereits an TARGET angeschlossen und Mitglied der EBA sein und über eine Mindest-Eigenkapitalausstattung von € 1,25 Mrd. verfügen.
- Ein Liquiditätspool bei der EZB in Höhe von 1 Mrd. Euro gewährleistet bei Ausfall einer oder mehrerer Parteien die Tagesendabwicklung offener Positionen.
- Ein Verlustaufteilungsverfahren („loss sharing scheme“) verteilt den eingetretenen Verlust im Schadensfall auf die beteiligten Banken.

4.2.3.5.3 STEP1

STEP1 und STEP2 sind Teil einer Initiative zur Förderung kosteneffizienter Zahlungsverkehrsabwicklungen im Bereich der Klein- und Geschäftskundenzahlungen im Euro-Raum S.T.E.P.S (Straight Through Euro Payment System).

STEP1 wurde im November 2000 in Betrieb genommen und ermöglichte den 90 teilnehmenden Banken über 5.000 BIC-Adressen direkt zu erreichen. Aktuell (Stand Sommer 2003) hat STEP1 bereits mehr als 270 Teilnehmer (114 reine STEP1-Banken, 6 aus Deutschland) und erreicht 9.000 BIC-Adressen.[199] Zugangsvoraussetzung zu STEP1 ist neben einer Mitgliedschaft bei der EBA eine Geschäftsverbindung zu einer EURO1-Bank, die vertraglich

[196] www.abe.org.
[197] Vgl. ausführlich 5.1.3.1.2.
[198] Vgl. www.abe.org.
[199] BdB (2003b), S. 43, EBA (2003).

abgesichert als so genannte Settlement-Bank für die STEP1-Bank auftritt. Zusätzlich muss das Personal der STEP1-Bank bei der EBA für die technischen Systeme und Prozeduren geschult werden.

Technisch ist STEP1 nichts anderes als eine Zugangsmöglichkeit zu EURO1 für Kreditinstitute, die nicht die aus Sicherheitsgründen hohen Zugangskriterien für EURO1 erfüllen. Es werden über STEP1 nur solche Zahlungen abgewickelt, die nicht systemkritisch werden können – vornehmlich Kundenzahlungen (direkt oder indirekt als Interbankenzahlungen im Kundenauftrag); die höchste Zahlung beträgt € 10 Mio., bereits ab € 1 Mio. werden spezielle Abstimmungsprozesse ausgelöst. STEP1 kann nicht als Massenzahlungssystem bezeichnet werden, da es auf EURO1 basierend die Abwicklung der Zahlungen einzeltransaktionsorientiert vornimmt.

STEP1 ermöglicht sowohl Überweisungen als auch bei Zustimmung des Geschäftspartners Lastschriften. Das System basiert auf dem SWIFT FIN-Service und verarbeitet analog zu EURO1 Zahlungen in den Nachrichtenformaten MT 100 (bis November 2003), MT 102, MT 103, MT 104, MT 202, MT 204 und MT 400. Für die Akzeptanz von MT 102, MT 104 und MT 204 sind bilaterale Abkommen notwendig, es besteht keine Pflicht, für Kreditinstitute, diese anzunehmen. Ein spezielle Kennzeichnung im SWIFT-Format (ERP (Euro Retail Payment in Feld 103 der Nachrichtenkopfzeile) ermöglicht es, STEP1-Zahlungen automatisiert zu erkennen.[200]

Zahlungen im STEP1-System werden von 7.30 Uhr bis 14.00 Uhr für den selben Tag angenommen und bis 16.00 Uhr verarbeitet, vorausgesetzt die Limitwerte der teilnehmenden Banken sind nicht überschritten. Eine reine STEP1-Bank kann zur Risikovermeidung keinen Negativsaldo haben, der nicht von einer EURO1-Bank gedeckt wird. Die operative Seite des Geschäfts wird über eine EURO1-Bank abgewickelt, so dass keine Schnittstellenproblematik entsteht. Als zusätzliche risikomindernde Maßnahme werden für STEP1-Banken individuelle Limits für die Empfänger- wie für die Senderseite zwischen € 1 Mio. und € 10 Mio. gesetzt.[201] Nach 14.00 Uhr werden die durch Zahlungen entstandenen Salden errechnet und mittels der für die jeweilige STEP1-Bank zuständigen Settlement-(EURO1)-Bank beglichen. Für entstehende Probleme bei einzelnen STEP1-Banken übernehmen die Settlement-Banken die Haftung.

Statistisch werden die STEP1-Zahlungen bei den EURO1-Zahlungen ausgewiesen (siehe 4.2.3.5.2), so dass über die Aktzeptanz von STEP1 am Markt keine Aussage getroffen werden kann.

4.2.3.5.4 STEP2

STEP 2, Teil des S.T.E.P.S-Programms, ist seit 28.04.2003 operativ tätig, und wird bereits als ein möglicher Vorläufer eines „Pan-European Automated Clearing House“ (PEACH) für Massenzahlungen im Bereich der Überweisungen – später eventuell auch der europäischen Lastschrift – gesehen.[202] Die Entwicklung von STEP2 wurde maßgeblich durch die Europäische Kommission getrieben, die mit der EU-Verordnung 2560/2001 im Rahmen der Vorbereitung für die gemeinsame Währung die Vorgabe machte, europäischen Auslandszahlungsverkehr preislich mit Inlandszahlungsverkehr gleichzustellen.[203]

[200] Vgl. www.abe.org.
[201] Vgl. EBA (2003), S. 2 f.
[202] Vgl. o.V. (2003d), o.V. (2003e).
[203] Vgl. Europäische Gemeinschaften (2001).

Das Henne-Ei-Problem – erst Investionen in ein kostengünstiges europäisches Massenzahlungssystem tätigen, wenn der europäische grenzüberschreitende Zahlungsverkehr ein hinreichend großes Volumen angenommen hat, und nicht ex ante – wurde für die Banken durch Regulierung „gelöst". Viner, Vize-Präsident der Boston Consulting Group in London, bringt es auf den Punkt:[204] „So to create change you either need a compelling economic case or you need a catalyst. The economic case is not that compelling…the volumes are not very great relative to domestic. […] The catalyst is the regulation and without that I don't think it would have happened at this time." Die Gültigkeit des "economies of scale"-Argumentes wird von anderen Autoren hingegen bezweifelt, die den grenzüberschreitenden Handel durch die hohen Kosten im Zahlungsverkehr behindert sehen.[205] Die Tatsache, dass ohne Regulierung keine durchgreifende Veränderung in kurzer Frist stattgefunden hätte, ist unumstritten.

Für die Zahlungen, die über STEP2 geleitet werden, gibt es klare Vorgaben, die der EU-Verordnung 2560/2001 entnommen sind – theoretisch könnten auch andere Zahlungen über diese Schiene laufen (nur könnten dann die dafür bislang höheren Gebühren nicht mehr durchgesetzt werden). Es sind Zahlungen möglich, die folgende Merkmale beinhalten:[206]

- es handelt sich um Überweisungen bis zu einer Höhe von € 12500,
- diese haben eine gültige International Bank Account Number des Begünstigten und
- einen gültigen Bank Identifier Code der Bank des Begünstigten und
- sie weisen den Gebührenschlüssel „SHA" (shared) auf.[207]

Es bestehen für die Kreditinstitute verschiedene Möglichkeiten, an STEP2 „anzudocken". Sie können entweder eigenständig als Mitglied direkt verbunden werden, bei einer Clublösung zusammen mit anderen Kreditinstituten über einen Knotenpunkt auf STEP2 zugreifen, oder über die Deutsche Bundesbank europäische Zahlungen verarbeiten. Neben anderen europäischen Zentralbanken wird die Deutsche Bundesbank direkt an STEP2 angebunden (siehe Abbildung 12). Als so genannter „country agent" übernehmen nationale Zentralbanken wie die Deutsche Bundesbank oder die italienische Banca d'Italia (aber auch Geschäftsbanken) die Funktion eines direkten Teilnehmers und lassen nationale Kreditinstitute als indirekte Teilnehmer an STEP2 zu. Desweiteren können nationale automatisierte Clearingstellen, betrieben von Finanzinstituten, als Anlaufstelle für Nicht-STEP2-Banken dienen, die auf diese Weise Zugang zum System bekommen. Ab dem 27.10.2003 werden somit grenzüberschreitende Euro-Massenzahlungen via EMZ der Deutschen Bundesbank europaweit möglich. Dabei sieht sich die Deutsche Bundesbank nicht als Wettbewerber der Großbanken sondern möchte lediglich wettbewerbsneutral den öffentlichen Kassen und kleineren Kreditinstituten einen indirekten Zugang zum europäischen Massenzahlungsverkehr ermöglichen.[208] STEP2-Zahlungen über die Deutsche Bundesbank werden per SWIFT-Format MT 103+ in den EMZ eingereicht und bezüglich der zeitlichen Priorität und Sperren wie andere Zahlungsvorgänge im EMZ behandelt. Eingehende Zahlungen liefert die Bundesbank taggleich an den Empfänger per DFÜ aus.

[204] o.V. (2003d).
[205] Vgl. Dennig (2002), S. 109.
[206] Vgl. Europäische Gemeinschaften (2001). Deutsche Bundesbank (2003f).
[207] Es werden die Gebührenschlüssel „OUR" (Auftraggeber übernimmt alle Gebühren), „BEN" (Empfänger trägt alle Gebühren) und „SHARE" (Kosten werden zwischen Auftraggeber und Empfänger aufgeteilt) unterschieden.
[208] Vgl. Deutsche Bundesbank (2003f).

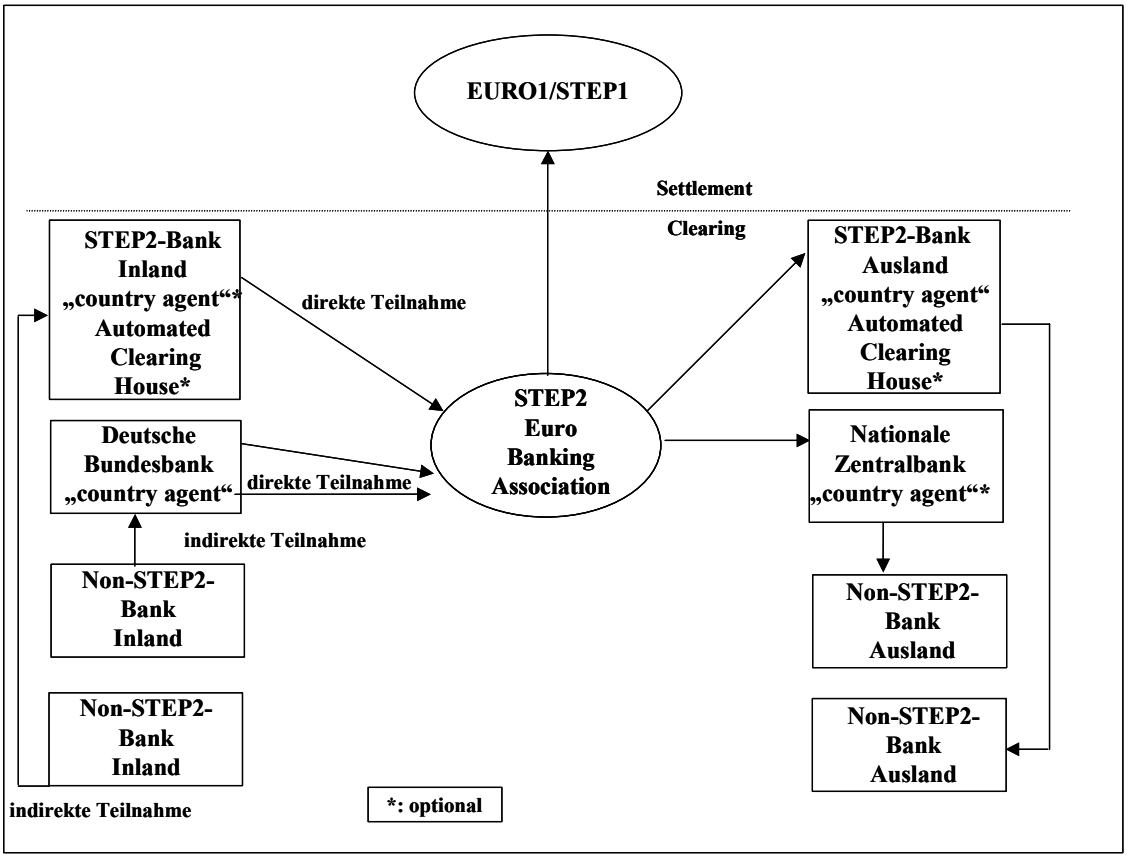

Abbildung 12: Zahlungsströme in STEP2 der Euro Banking Association[209]

Die Betreiber bezeichnen STEP2 als ein auf höchstem Sicherheitsniveau arbeitendes Zahlungssystem.[210] Unter anderem werden die Sicherheitsmerkmale der Zahlungsnachrichten im System bei Eingang überprüft. Kommt es zu unschlüssigen Ergebnissen, wird die Zahlung abgewiesen.[211] Zusätzlich trägt, trotz Massenzahlungssystem, jede Zahlungsanweisung eine eindeutige Transaktions-Referenznummer.

Die direkten Teilnehmer an STEP2 haben die Möglichkeit, den Status der von ihnen direkt oder indirekt in Auftrag gegebenen Zahlungen online über ein Informationssystem zu überprüfen.[212]

4.2.4 Nachrichtenübermittlungssystem SWIFT und SWIFT-Dienstleistungen

Grundlage für sicheren Zahlungsverkehr ist ein sicherer Informations-/Nachrichtenaustausch. Dieser wird im internationalen Zahlungsverkehr, zunehmend in Europa auch im nationalen Bereich, durch die „Society for Worldwide Interbank Financial Telecommunication“ (S.W.I.F.T. SCRL)[213] gewährleistet.

[209] Eigene Darstellung auf Grundlage Deutsche Bundesbank (2003e), S. 3 ff., BdB (2003b), S. 71.
[210] EBA (2002), S. 5.
[211] EBA (2002), S. 9.
[212] Vgl. EBA (2002), S. 19.
[213] Sowohl die Dienste als auch das Unternehmen werden im folgenden mit SWIFT abgekürzt.

4.2.4.1 S.W.I.F.T. SCRL

SWIFT wurde 1973 in Brüssel von der Finanzindustrie gegründet, um ein gemeinsames Datenverbundsystem mit internationalen Standards zu schaffen, mit dessen Hilfe eine schnellere, rationellere und einheitlichere Abwicklung internationaler Zahlungsströme erfolgen sollte. Zusätzlich sollten weitere Nachrichten zwischen Kreditinstituten zuverlässig übermittelt werden. Hauptsitz des Unternehmens ist La Hulpe in Belgien. Das System hat heute 7.455 Teilnehmer in 199 Ländern (Stand Sommer 2003). SWIFT ist als Aktiengesellschaft im Besitz von über 3.000 Finanzinstituten. 2002 wurden mit 1.647 Mitarbeitern 1,8 Mrd. Nachrichten (Zahlungsinformationen, Wertpapiermitteilungen, Handelsmitteilungen, Schatzanweisungen) übermittelt und täglich Zahlungsnachrichten von über 5.000 Mrd. US-Dollar verarbeitet.[214] Der Markt für Zahlungsnachrichten ist das wichtigste Standbein mit über 1 Mrd. Operationen im Jahr 2002 und fast 20 % Wachstum per annum. SWIFT ist die Nachrichtenplattform für weltweit über 40 Zahlungssysteme.

Im Zahlungsverkehr ist SWIFT in drei Bereichen tätig.[215] Für den Großzahlungsverkehr ist das erste Segment von Bedeutung. Dort stellt SWIFT das Kommunikationsnetzwerk für den Betrieb der Systeme zur Verfügung. Einen zweiten Bereich umfassen Netzwerke für Finanzinstitute, die untereinander kommunizieren wollen. Zunehmend versucht SWIFT sich auch im Bereich Kunde-Bank zu etablieren, beispielsweise mit einem eigenen Zahlungssystemangebot e-paymentsPlus.

SWIFT betreibt als Dienstleister ein weltweit verfügbares Nachrichtensystem für den Finanzbereich und wickelt über 90 % der Informationen des internationalen Finanzverkehrs ab. Die Schnelligkeit der Datenübertragung liegt weltweit bei unter 20 Sekunden.

Die technisch/organisatorische Infrastruktur ist bei SWIFT dreistufig:[216]

1) Auf der obersten Ebene finden sich zwei spiegelbildlich ausgelegte Hochverfügbarkeitsrechenzentren (Operating Center (OPC)) in Zoeterwoude (Niederlande) und Culpeper (USA). So genannte Slice Processors bündeln die Informationen der darunter liegenden Ebene.
2) Die mittlere Ebene bilden regionale Knotenpunkte (Regional Processor).
3) Auf der Kunden-(Bank)-Ebene sind diese mit Terminals an die Regional Processors angebunden.

SWIFT ist jedoch selbst kein Zahlungssystem, sondern ein Nachrichtenübermittlungssystem, das für die Zahlungssysteme eine wichtige Rolle spielt. Finanztransaktionen werden weiterhin über die Konten und Systeme der beteiligten Finanzinstitutionen abgewickelt. Den wohl gewichtigsten Vorteil von SWIFT beschreibt anschaulich Stephan Zimmermann von der UBS AG[217]: „I think the unique value of SWIFT is that it is owned by all the banks in the world. It can not only set standards, but implement and execute them. That's a unique proposition nobody else has." Durch die Quasi-Monopolstellung im Bereich der Nachrichtenübermittlung wird es SWIFT möglich Standards, die international akzeptiert werden, einzuführen. Beispielsweise zeichnet SWIFT für die Entwicklung und Verwaltung des so genannten Bank Identifier Codes (BIC) verantwortlich. Der BIC ist das internationale Pendant zur deutschen Bankleitzahl. Für die ebenfalls von SWIFT vorangetriebenen Straight-Through-Processing-Ansätze ist der BIC in Kombination mit der vom European Committee for Banking Standards

[214] Vgl. SWIFT (2003a).
[215] Vgl. http://www.swift.com/index.cfm?item_id=2325 (29.08.2003).
[216] http://www.zahlungsverkehrsfragen.de/swift.html., Riedl (2002), S. 44 f.
[217] SWIFT (2003a), S. 19.

(ECBS) entwickelten International Account Number (IBAN) eine wichtige Grundlage, um international jedes Kreditinstitut eindeutig ansprechen zu können.

4.2.4.2 Nachrichtenübermittlung via SWIFT

Die Übermittlung von Daten erfolgt in Form sogenannter Message Types (MT). Message Types werden zur Übermittlung von Zahlungsaufträgen verwendet, die in den gängigen Zahlungssystemen von Bedeutung sind. Die Message Types geben in der ersten Ziffer die Nachrichtenkategorie an: zum Beispiel steht 1 für Nachrichten zu End-Kundenzahlungen, 2 für Interbankenzahlungen, 4 sind Dokumenteninkassi, 9 Cash-Managementnachrichten. Die zweite Ziffer gibt die Nachrichtengruppe, die dritte den spezifischen Nachrichtentyp an. Im Einzelnen sind im Individualzahlungsverkehr folgende MT von Bedeutung:

- MT 100 Kundenüberweisung (läuft am 15. November 2003 aus)
- MT 102 Kundenüberweisung als Sammelauftrag
- MT 102+ Sammelzahlungsauftrag
- MT 103 Einzelne Kundenüberweisung (ersetzt MT 100 ab November 2003)
- MT 103+ einziges STP-fähiges SWIFT-Format. Es handelt sich um ein um STP[218]-störende Details reduziertes MT 103 Format.
- MT 104 Kundenlastschriften/Cash Management
- MT 121 Banküberträge als Sammelauftrag
- MT 199 Freies Format (Textnachricht)
- MT 202 Allgemeiner Übertrag zwischen Finanzinstitutionen
- MT 204 Gebührenverrechnung, Scheckeinzug und Dokumentengeschäft
- MT 205 Ausführung eines Bankübertrages
- MT 400 Bezahltmeldung eines Inkassoauftrages mit Verrechnung des Gegenwertes

Im nationalen Zahlungsverkehr spielen die SWIFT-Formate noch eine untergeordnete Rolle. Aus Effizienzgründen kann vermutet werden, dass in Europa zunehmend die Vielzahl nationaler Formate, die beim grenzüberschreitenden Zahlungsverkehr konvertiert werden müssen, vereinheitlicht wird. SWIFT bietet sich in diesem Zusammenhang an. Allerdings spricht die Kostenstruktur bislang noch gegen den vermehrten Einsatz von SWIFT im nationalen Umfeld, es ist teurer als beispielsweise das deutsche Datenträgeraustauschformat (DTAUS).[219] Die Kosten sinken allerdings mit zunehmender Nutzung der SWIFT-Dienste und dem Einsatz neuer Technologien seit Jahren. In den letzten 10 Jahren sind die Preise für SWIFT-Nachrichtendienste um 70 % gesenkt worden.[220]

Bei den SWIFT-Diensten sind die SWIFT FIN-Dienste für die Zahlungssysteme relevant. Seit 1977 werden diese Dienste nach dem „store-and-forward"-Prinzip[221] der Nachrichtenübermittlung basierend auf dem X.25-Protokoll[222] angeboten. Neben der reinen Datenübertragung werden bei den FIN-Diensten die Nachrichtentypen auf ihre Syntax überprüft und im Fehlerfall Meldungen weitergeleitet. Zusätzlich lassen sich Auslieferungsprotokolle, Dringlichkeitsstufen, Speichermöglichkeiten und Suchfunktionen in FIN realisieren. Im Rahmen des Übergangs auf SWIFTNet, mit Pilotprojekten seit 2001, im Massenbetrieb seit

[218] STP: Straight Through Processing.
[219] BdB (2003b), S. 55.
[220] Http://www.swift.com/index.cfm?item_id=41322 (29.08.2003).
[221] Eine Nachricht wird über einen Server geschickt und dort so lange gespeichert (store), bis der Empfänger identifiziert und empfangsbereit ist, dann erst wird sie weiter geschickt (forward).
[222] Protokoll zur Kommunikation in Datennetzen, erstmals 1976 spezifiziert, Nachfolger sind beispielsweise TCP/IP, die neben der reinen Datenübertragung auch Zusatzdienste ermöglichen.

Mitte 2002, werden nunmehr die heute üblichen Protokolle genutzt, die mehr Komfort und Sicherheit ermöglichen.

Der FIN Copy-Dienst ist ein zusätzlicher SWIFT FIN-Dienst, der es ermöglicht, im Bereich von Großzahlungen und im Wertpapierhandel eine Kopie der Zahlungsnachricht zunächst von einem Server autorisieren zu lassen, bevor die Zahlung nach erfolgreicher Bestätigung weiterverarbeitet wird.

Die Details der Absicherung der SWIFT Dienste, Secure Login and Select (SLS), sowie Bilateral Key Exchange (BKE) und SecureX25 encryption device sind öffentlich nicht verfügbar.[223] Bekannt ist lediglich, dass für die Nachrichtenübermittlung zwischen zwei Kommunikationspartnern bilateral ausgetauschte Schlüsselpaare verwendet werden (symmetrische Verschlüsselung). Darauf basiert die Authentifizierung der Nachrichtenübermittlung, die durch den so genannten Message Authentification Code (MAC), oder Proprietary Authentification Code (PAC) für FIN Copy-Dienste gewährleistet wird. Zwischenfälle im Zusammenhang mit Betrug oder Manipulation von Nachrichten sind aus der langen Betriebszeit von SWIFT von 1977 bis 2003 nicht öffentlich bekannt geworden (siehe auch 5.3.2.1.2).

Die Zuverlässigkeit der SWIFT-Dienste ist laut eigenen Angaben der Organisation nahe 100 %. Sie betrug 2002 für die SWIFT FIN-Dienste 99,996 %, für das reine Datentransportnetzwerk 99,995 % und für alle Dienste zusammen 99,991%.[224] Das System ist so ausgelegt, dass der Ausfall einzelner Regional Prozessoren innerhalb von höchstens vier Minuten geschehen kann; zwischen den beiden Zentralrechnern der Operating Centers kann bei Problemen innerhalb von maximal 30 Minuten gewechselt werden.[225] SWIFT gibt an, während der Vorgänge um den Terrorangriff von New York am 11. September 2001 keinerlei Ausfälle oder Qualitätseinbußen im eigenen Netz gehabt zu haben.[226]

4.2.4.3 SWIFTNet

Die neue Architektur SWIFTNet, die so schnell wie möglich die bisherige Infrastruktur ersetzen soll, bietet neue Dienste und integriert die bestehenden Dienste, im Zahlungsverkehr insbesondere die SWIFT FIN-Dienste. Dabei ändern sich die Transportkanäle, die Nachrichtentypen (MT) und BIC bleiben unverändert. Wesentliche Veränderungen gibt es durch die Zugangsmöglichkeiten auf der Infrastrukturebene mittels der neu eingeführten VPN Box (Virtual Private Network). Die VPN Box, verwaltet von SWIFT, sorgt für verschlüsselte Sicherheit auf Netzwerkebene mittels Public Key Infrastructure (PKI) und übernimmt das Senden und Empfangen von Nachrichten über IPsec-Tunnel (ein Industriestandard, der einen verschlüsselten Datentransport auf gesichertem Weg ermöglicht).

SWIFTNet ist eine (IP)-basierte Nachrichteninfrastruktur, die anstelle der alten X.25-Verbindungen auf dem SWIFT Secure IP Network (SIPN) aufbaut.[227] SWIFT bedient sich dabei zusätzlicher Netzwerkpartner (AT&T, Colt, Equant, Infonet), die es den Kunden ermöglichen, Zugang zu einem SIPN-Backbone zu erhalten. Die Sicherheit der Datenübertragung wird über SWIFT-Software gewährleistet: SWIFTNet Link (die Software zur Nutzung der PKI) und die SWIFTNet Public Key Infrastructure. Die SIPN-Backbones sind der Zugang zu SWIFT Operating Centres, den Zentralrechnern.

---

[223] Vgl. SWIFT (2003b), S. 10 und S. 17.
[224] Http://www.swift.com/index.cfm?item_id=4329 (29.08.2003).
[225] Vgl. Riedl (2002), S. 45.
[226] Vgl. http://www.swift.com/index.cfm?item_id=41749 (29.08.2003).
[227] Vgl. SWIFT (2003b), S. 9 ff.

Die Struktur einer Nachricht wird bei SWIFTNet um eine verschlüsselte Meta-Informationsebene ergänzt. Sind SWIFT FIN-Nachrichten durch einen FIN header gekennzeichnet, der quasi als Adresse der in einem „Umschlag“ verpackten Nachricht gilt, wird bei SWIFTNet zusätzlich dieser adressierte Umschlag in einen neuen Umschlag gepackt und mit einem SWIFTNet FIN header versehen. Dieser header umfasst neben der Adresse der sendenden auch die empfangende Institution, den Nachrichtentyp, den Namen des Dienstes und die IP-Adressen.[228] Die Verschlüsselung einer Nachricht findet auf der SWIFTNet Link-Ebene statt, die gesicherte Verbindung ins Netzwerk garantiert die SWIFTNet PKI.

Die neue Sicherheitsinfrastruktur in SWIFTNet soll dazu beitragen, die hochgesteckten Sicherheitsziele im System zu erreichen:[229]

- Zugang nur für registrierte SWIFTNet Kunden,
- Datenintegrität gesichert,
- Daten sind nur für Empfänger lesbar,
- die Identifizierung der Teilnehmer ist gesichert,
- die Authentizität des Absenders ist überprüfbar und
- die Nichtabstreitbarkeit eines Nachrichtenaustauschs ist gewährleistet.

Den Umgang mit der neuen Technologie auf Sicherheitsseite müssen die jeweiligen IT-Sicherheitsverantwortlichen bei SWIFT-Schulungen erlernen. Sie sind verantwortlich für die lokale Passwort- und Schlüsselverwaltung für die gesicherten Zugänge.

Auf SWIFT-Ebene wird ein unabhängiges Security Management Centre (SMC) betrieben. Das SMC übernimmt unter anderem die Überprüfung der Systemsicherheit, erzeugt die Passwörter für die Netzwerkzugänge, führt das für die PKI notwendige Zertifikatsverzeichnis, gibt Security Tokens, z. B. Smartcards zur Systemverwaltung, aus und ist für das Notfallmanagement zuständig, beispielsweise Sperren von Zertifikaten. Zusätzlich werden die Maßnahmen von unabhängigen Gutachtern überprüft und in einem Sicherheitsbericht veröffentlicht.[230]

4.2.5 Risiken im Interbankenzahlungsverkehr

Die Darstellung der Interbankenzahlungsverkehrs-Landschaft hat die vielfältigen Möglichkeiten gezeigt, mit denen grenzüberschreitender aber auch nationaler Zahlungsverkehr in Europa abgewickelt werden kann. Diese Vielfalt hat für die Sicherheit zwei Seiten: Einerseits entstehen (kostenintensive) Redundanzen, die im Fall von Systemstörungen helfen, dieses zu stabilisieren, andererseits nehmen die Angriffs- und Manipulationsmöglichkeiten und ebenso resultierende Systemfehler stark zu, wenn parallel verschiedenste Systeme betrieben werden. Die Mitarbeiter werden in diesen Fällen mit verschiedenen Prozeduren mehr oder weniger vertraut. Die weniger verwendeten Verfahren geraten dabei eher in Vergessenheit und können zu Manipulationen missbraucht werden.

Die beispielhaften Schadensfälle in Kapitel 5.3.2.1 zeigen, dass das Risiko von Betrugsfällen zunimmt, wenn keine standardisierten Prozesse eingesetzt werden, die zudem der ständigen Aktualisierung von Sicherheitsmaßnahmen technischer und organisatorischer Art unterliegen.

[228] Vgl. SWIFT (2003b), S. 15 f.
[229] Vgl. Münch (2002), S. 116.
[230] Vgl. Münch (2002), S. 119 f.

Die zunehmende Beseitigung systemischer Risiken im Großzahlungsverkehr ist nicht zuletzt durch die Abkehr der Zahlungssystembetreiber, insbesondere den Zentralbanken, von Netto-Abwicklungssystemen zu erklären. Diese Entwicklung ist aus Kosten- und Wettbewerbsgesichtspunkten in Europa aber keinesfalls unumkehrbar. Beispielsweise befürchtet Fabritius für den Fall, dass es nicht gelingt, TARGET und die angeschlossenen nationalen Brutto-Zahlungsverfahren technisch zu konsolidieren und wettbewerbsfähig mit privaten Anbietern zu halten, eine Umkehr des Trends zu Bruttosystemen, und damit eine Zunahme des systemischen Risikos.[231]

Aus technischer Sicht ist der zunehmende Einsatz international gebräuchlicher Nachrichtenformate auch auf nationaler Ebene, beispielsweise die SWIFT-IPsecure-Technologie, ein Garant für mehr Sicherheit. Dies gilt nicht so sehr, weil in der Vergangenheit technische Angriffe erfolgreich waren (Kapitel 5.3.2.1 zeigt eher die bisherige „Unangreifbarkeit" der technischen Infrastruktur) sondern vielmehr für die zukünftige Entwicklung. Es kann davon ausgegangen werden, dass die Informationsgesellschaft zunehmend auch die kriminellen Energien in IT-Kanäle lenkt, die bisher von solchen Aktivitäten weitgehend verschont geblieben sind. Insofern zählt der Aufbau kryptographischer Infrastrukturen zu den präventiven Maßnahmen der Betrugsbekämpfung.

Die Übermittlung der Nachrichten innerhalb der Zahlungsverkehrsnetze gilt als ein sensibler Punkt bei möglichen Angriffen. Auch wenn mit der SWIFTNet-Architektur offene Netze genutzt werden, zeigt sich, dass die Sicherheitsmaßnahmen mittels virtuellen privaten Netzen innerhalb offener Netze zu gleicher Sicherheit wie in geschlossenen Netzen führen. De facto sind solche Konstruktionen wie SWIFTNet geschlossene Netze. Damit reduziert sich auch die Anzahl potenzieller Angriffe auf das Nachrichtennetz erheblich. Von außen lassen sich Störungen der Infrastruktur noch am ehesten Vorstellen, sei es in Form so genannter Denial-of-Service Attacken oder die physische Zerstörung von Leitungen. Ohne Innentäter wird es bei der neuen Konstruktion von SWIFTNet kaum möglich sein, Nachrichten abzuhören oder gar zu manipulieren. Einzig, wenn an den Endpunkten der Verschlüsselung Täter die Möglichkeit zur Manipulation der beteiligten Rechner bekämen, könnten Schäden entstehen; im schlimmsten Fall wäre eine Manipulation des Rechners via Internet möglich.[232]

Bei den Großzahlungssystemen steht die Sicherung der Systeme ebenfalls an hoher Stelle der Prioritätenliste. TARGET gilt bereits aufgrund System-Eigenschaften, z. B. der Echtzeitübertragung von Zentralbankgeld, als sehr sicheres System, das die Gesamtheit der Abwicklungsrisiken im Euro-Zahlungsverkehr minimiert. Über redundante Systeme werden Sicherungskopien möglich, die bei Systemteilausfällen eine schnelle Rückkehr zum normalen Geschäftsbetrieb ermöglichen. Die veröffentlichten Störungen ließen sich auf Softwarefehler oder sonstige Probleme mit Hard- oder Software, aber auch auf Streiks zurückführen; kriminelle Handlungen haben nicht zu (veröffentlichten) Problemen geführt. Mittels Informationssystem können die anderen Teilnehmer bei Störungen einzelner Komponenten unterrichtet werden und alternative Wege für ihre Zahlungen verwenden, beispielsweise Korrespondenzbankbeziehungen. Die Schwierigkeit liegt bei größeren Störfällen eher in der begrenzten Bearbeitungskapazität bei der dann folgenden manuellen Bearbeitung der Zahlungseingänge. Vorteilhaft wirkt sich jedoch der relativ geringe Teilnehmerkreis größerer Banken mit systemkritischen Zahlungen aus. Im Störungsfall können Probleme durch direkte Kontaktaufnahme und Ad hoc Entscheidungen gelöst werden.

[231] Vgl. Fabritius (2001), S. 11 f.
[232] Vgl. Münch (2002), S. 130 f.

Der dezentrale Aufbau des jetzigen TARGET-Systems ist jedoch neben Kosten- auch unter Sicherheitsaspekten umstritten.[233] Nationale Interessen haben bislang eine einheitliche Lösung im Sinne von TARGET2 verzögert. Dennoch kommt beispielsweise der Bundesverband deutscher Banken zu der eindeutigen Schlussfolgerung:[234] „Erst auf der Basis einer gemeinsamen, einheitlichen und zentralen technischen Plattform lassen sich das Krisenmanagement, die Notfallplanungen und somit die Krisensicherheit des zukünftigen Systems substanziell verbessern und operative Aspekte harmonisieren." Beispielsweise sind bislang die nationalen Zugänge zu den RTGS-Systemen unterschiedlich gesichert und könnten zum Ziel von Angriffen, unter anderem Denial-of-Service-Attacken werden.[235] Es steht zu vermuten, dass ein Redesign von TARGET hin zu TARGET2 analog zu der bei SWIFT FIN und SWIFTNet durchgeführten Aktualisierung der technischen Sicherheitsgrundlagen zu mehr Sicherheit führen wird.

Das zweite bedeutende Großzahlungssystem in der Europäischen Union, EURO1, weist im Kern die gleichen Probleme des Netzzugangs auf wie TARGET. Allerdings ist das Design weniger komplex, und bei den hohen Eintrittsschranken handelt es sich de facto weniger um ein offenes als ein geschlossenes System (Clublösung). Die Risiken sind nicht zuletzt aufgrund vertraglicher Regelungen klar begrenzt. Kriminelle Manipulation ist durch die einheitlichen Verfahren, die auf SWIFT-Nachrichten basieren und in einem geschlossenen Netz ablaufen, wiederum nur durch Innentäter denkbar, oder durch den kaum vorstellbaren Zugriff eines Außentäters auf einen Zugangsrechner. EURO1 gilt in Bezug auf die Erfüllung der Lamfalussy-Kriterien als ideales Großzahlungssystem. Riedl weist gleichwohl nach, dass es unter Umständen zu systemischen Problemen kommen kann (Gridlock[236]), da die Innertagesliquiditätssteuerung zu schwach ausgelegt ist[237] – die Problematik der Liquiditätssteuerung bei Zahlungssystemen ist allerdings nicht Gegenstand dieser Arbeit.

Höhere Risiken birgt aus Sicherheitsgesichtspunkten das Korrespondenzbankensystem. Es hat bereits mehrfach zu öffentlich bekanntgewordenen Schadensfällen geführt.[238] Das Grundproblem liegt in den heterogenen Ansätzen der Sicherungsmaßnahmen. Eigenlösungen können teilweise sehr wirksam sein, teilweise werden Lücken, die bei standardisierten Verfahren schneller entdeckt und beseitigt werden können, erst bei realisierten Schadensfällen offensichtlich.

4.2.6 Retail-Bezahlverfahren in Deutschland

In den vorangehenden Abschnitten wurde die Zahlungssystem-Infrastruktur aus Sicht der Kreditinstitute vornehmlich im Interbankenzahlungsverkehr dargestellt und zwischen Individual-Zahlungssystemen für Großbeträge und dem Massenzahlungsverkehr unterschieden. Im folgenden Abschnitt werden die Zahlungssysteme beschrieben, die für Kunden-Bank- und Kunden-Händler-Beziehungen vornehmlich im Bereich elektronischer Handel eingesetzt werden.[239] Der Einsatz dieser Systeme stößt neben den Zahlungsverfahren im Einzelhandel, Großhandel und im Business-to-Business-Sektor[240] Zahlungsströme im Massenzahlungsverkehr der Kreditwirtschaft an.

---

[233] Vgl. Riedl (2002), S. 179 ff., Fabritius (2001), S. 8.
[234] BdB (2003b), S. 35.
[235] Vgl. Münch (2002), S. 134.
[236] Systemilliquidität, bei der ein Teilnehmer an der Durchführung von Zahlungen gehindert werden, da andere Teilnehmer nicht zahlen können. Vgl. Riedl (2002), S. 93.
[237] Vgl. Riedl (2002), S. 207f.
[238] Siehe z. B. 5.3.2.1.2.
[239] Die Ausführungen basieren im Wesentlichen auf Leibold (2003), ergänzt um Aktualisierungen.
[240] Hier unter Umständen auch Individualzahlungsverkehr.

4.2.6.1 Kategorisierung der (Internet-)Bezahlverfahren im B2C-Bereich

Die Kategorisierung von Bezahlsystemen im B2C-Bereich kann nach unterschiedlichen Kriterien geschehen, beispielsweise nach der Höhe der transferierten Beträge oder nach dem Bezahl-Zeitpunkt. Aus der Sicht des Kunden wie des Händlers ist der Zeitpunkt des Übergangs des Geldes von Kunde zu Händler/Bank von Interesse. In Abbildung 13 werden die aktuellen Zahlungssysteme (nicht nur) im Internet nach diesem Kriterium kategorisiert. Es werden Pay-before-Verfahren, Pay-now- und Pay-later-Varianten unterschieden.

Bei Pay-before-Verfahren erhält der Händler sein Geld vor Übertragung der physischen oder digitalen Waren und Dienstleistungen. Die gängigen Verfahren in Deutschland beinhalten, dass der Kunde bereits vorher bei einem Zahlungssystemanbieter, beispielsweise der Deutschen Telekom AG, eine beliebige Summe einzahlt und im Gegenzug ein „Guthabenkonto" für verschiedene Einsatzmöglichkeiten erhält, respektive freischaltet. Dieses Guthaben wird momentan nicht verzinst und stellt insofern eine Parallele zum Bargeldbesitz dar – mit teilweise besserer Absicherung(smöglichkeit).

Die Pay-now-Systeme zeichnen sich durch den (fast) zeitgleichen Übergang des Geldes und der Ware aus. Das bekannteste Verfahren stellt die klassische Nachnahme dar, bei der der Empfänger der notwendigerweise physischen Ware dem überbringenden Dienstleister Bargeld bei Warenerhalt aushändigt – genau betrachtet ist das Geld damit noch nicht auf dem Konto oder in der Hand des Empfängers.

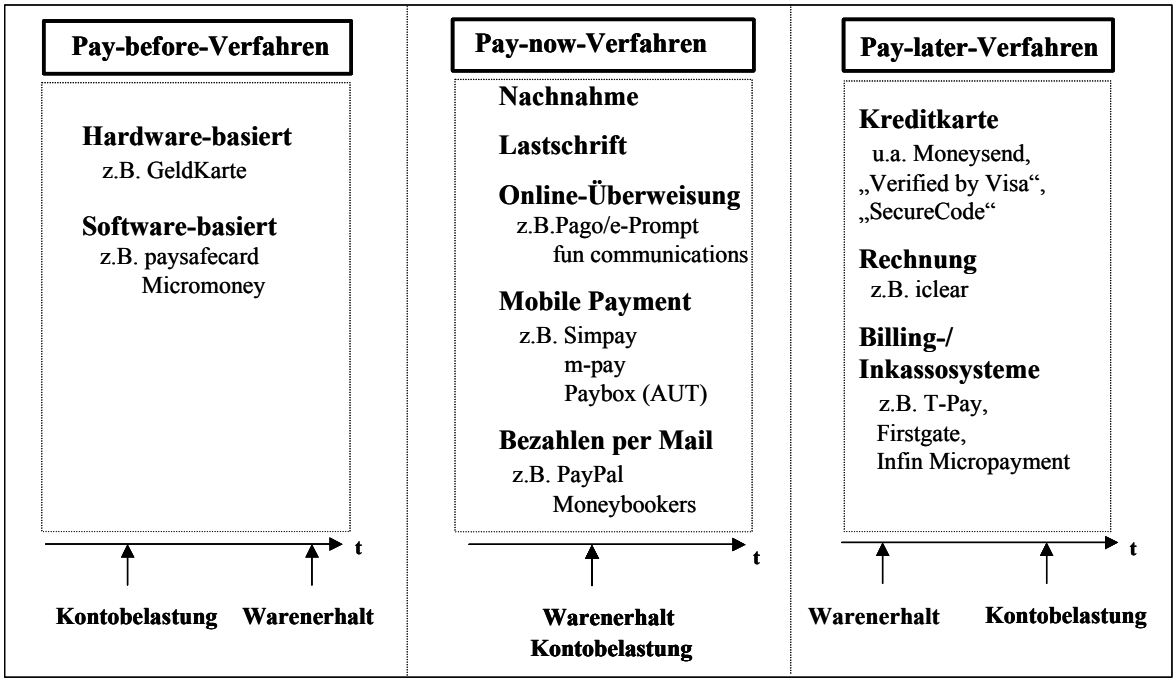

Abbildung 13: Kategorisierung der Internet-Bezahlverfahren im B2C-Segment[241]

Die Pay-later-Bezahlverfahren ermöglichen dem Käufer zunächst die bestellte Ware zu begutachten, bevor das Geld von seinem Konto (Kreditkarte, Girokonto) abgebucht wird – mit entsprechenden Möglichkeiten der Zahlung sowohl berechtigt als auch unberechtigt zu widersprechen. Die nächsten Abschnitte beschäftigen sich mit den Zahlungssystemkategorien

[241] Eigene Darstellung in Anlehnung an Leibold (2003).

und Wirkungsprinzipien, in Abschnitt 4.2.6.5 wird auf Risiken im Retail-Bezahlbereich eingegangen.

Die Kategorisierung nach dem Bezahlzeitpunkt ist unter anderem wegen den Interbanklaufzeiten einer Zahlung nicht ohne Unschärfen. Wird beispielsweise bei der Online-Überweisung die einmal autorisierte Überweisung taggleich und ohne Widerrufsmöglichkeit durchgeführt, handelt es sich in der Tendenz um ein Pay-now-Verfahren. Beträgt die Laufzeit hingegen drei Tage und ist die Zahlung unter Umständen vom Kunden zurückrufbar, fällt das Verfahren in den Bereich der Pay-Later-Systeme.

Die technische Entwicklung lässt den Bezahlzeitpunkt tendenziell näher an den Übergabezeitpunkt rücken. Für den Anbieter von digitalen Waren und Dienstleistungen im Internet eine konsequente Weiterentwicklung, die das Bezahlrisiko senkt, für den Kunden, der sich an Pay-later-Mechanismen gewöhnt hat, eine unvorteilhafte Entwicklung. Unberührt bleibt von der Frage des Bezahlzeitpunktes die Frage der Verbraucherrechte bei Mail-order/Telephone-order Geschäften.

4.2.6.2 Pay-before-Verfahren

4.2.6.2.1 Vorausbezahlte Karten (Prepaid-Karten)

Die vorausbezahlten Telefonkarten und ihr Erfolg können als Vorläufer für die Entwicklung vorausbezahlter Zahlungssysteme gesehen werden. Telefonkarten werden nicht als Zahlungsmittel gesehen, da sie nicht zu unterschiedlichen Zwecken eingesetzt werden können. Demgegenüber sind Prepaid-Karten, die in Deutschland 2003 von zwei Anbietern auf dem Markt sind, als Zahlungsmittel einsetzbar. Die paysafecard wird von der d.paysafecard.com GmbH (Tochergesellschaft der österreichischen Paysafecard.com Wertkarten AG) und die Micromoney-Karte von der Deutschen Telekom Tochter DeTeCardService angeboten. Der Einsatzzweck als Zahlungsmittel gilt als bankerlaubnispflichtiges Geschäft und erfordert, dass ein besonderes rechtliches Konstrukt gewählt werden musste, bei dem ein Finanzinstitut (Commerzbank AG und Postbank AG) durch einen Geschäftsbesorgungsvertrag treuhänderisch das vorausbezahlte Geld der Kunden verwaltet.

In Deutschland sind die vorausbezahlten Karten paysafecard und MicroMoney-Card als so genannte Scratch-Karten ausgeführt, bei denen durch Freirubbeln und die Eingabe einer 16-stelligen PIN die Karte erst freigeschaltet wird. Beide Karten haben neben der Möglichkeit einzukaufen auch die Telefonoption, bei der MicroMoney-Card mit einer weiteren PIN, die es freizurubbeln gilt, bei der paysafecard mit der gleichen PIN über einen „Einkauf“ beim Telefonanbieter analog zu sonstigen Einkäufen. Die PIN wird lediglich durchs Telefon übermittelt. Die paysafecard existiert in zwei Varianten, eine rote Karte ist für jeden erhältlich, die blaue Karte ist für Käufer über 18 Jahre reserviert.

Der Einkaufsvorgang läuft grundsätzlich wie folgt ab: Nach dem Kauf wird die PIN im Internet eingegeben (SSL-verschlüsselt wie auch alle anderen Transaktionen, die über den Server des Systemanbieters laufen, z. B. Kontostandsabfrage), der Server des Anbieters eröffnet für die intern validierte PIN ein Guthabenkonto, das bei jedem erfolgreichen Einkauf neu berechnet wird. Für den Kunden entstehen keine Kosten durch den Einkaufsvorgang, diese fallen beim Händler an. Der Anbieter des Zahlungssystems rechnet in bestimmten Zeitabständen mit den Händlern die angefallenen Beträge ab und überweist auf herkömmlichem Bankweg die entsprechenden Summen.

Sicherheit entsteht bei vorausbezahlten Karten auf mehreren Wegen. Zunächst ist der Verlust bei diesen Karten bereits durch den Maximalbetrag der Karte (100 Euro) begrenzt. Bei der paysafecard kann neben der PIN bei der Aktivierung des Guthabens durch den Käufer ein zusätzlicher Passwortschutz gewählt werden, bei dem der Käufer ein beliebiges Passwort wählt. In diesem Fall kann bei Verlust oder Diebstahl niemand ohne Kenntnis des Passwortes an das Guthaben gelangen. Der Kunde erhält sein Geld jedoch nur, wenn er selbst noch eine Kopie der PIN besitzt, ansonsten fällt im obigen Fall das Geld an den Treuhänder zurück. Die Möglichkeit einer Umsatzübersicht gibt den Käufern zusätzliche Sicherheit, da die abgebuchten Beträge mit dem Kaufpreis verglichen werden können. Um weitere Sicherheit zu gewährleisten verzichtet beispielsweise MicroMoney auf den Einsatz von Cookies, Java-Applets und Plug-Ins, die für Hacker eine relativ einfache Möglichkeit bieten könnten, an Daten des Käufers zu gelangen, beispielsweise mittels Cross-Site-Scripting[242]. Nachteilig für die Käufer kann sich die bei Scratchkarten fehlende Rückbuchungsmöglichkeit bei Reklamationen erweisen, hier müssen sich Kunde und Händler bilateral einigen.

Mittlerweile kommt es zu Kombinationen verschiedener Systeme, beispielsweise können Paylater-Systeme wie ein Firstgate-Benutzerkonto mit Prepaid-Funktionalitäten versehen werden. Dazu wird das Benutzerkonto beispielsweise über Kreditkarte aufgeladen.

4.2.6.2.2 GeldKarte

Die GeldKarte ist eine institutsübergreifende elektronische chipkartenbasierte Geldbörse der deutschen Kreditwirtschaft. Die Geldeinheiten auf der GeldKarte entsprechen als einziges Zahlungsmittel in Deutschland – nach der Einstellung des Betriebs von eCash und CyberCash – elektronischem Geld im Sinne der EG-Richtlinie 2000/46[243]. Der Aufbau und Betrieb des Systems „GeldKarte“ wird von den vier großen kreditwirtschaftlichen Verbänden in Deutschland – Bundesverband deutscher Banken e. V. , Deutscher Sparkassen- und Giroverband e. V., Bundesverband der deutschen Volksbanken und Raiffeisenbanken e. V. und Bundesverband Öffentlicher Banken Deutschlands e. V. – gewährleistet, die zu diesem Zweck eine ZKA-Vereinbarung geschlossen haben. Das Zahlungssystemprodukt GeldKarte ist seit 1996 am Markt präsent. Entscheidungen über die Entwicklung der GeldKarte und der dazugehörigen Infrastruktur werden von den beteiligten Verbänden gemeinsam im ZKA getroffen. Die Frage, welches Kreditinstitut auf seinen Karten den Chip anbietet, bleibt den einzelnen Häusern überlassen. Stand Sommer 2003 sind in Deutschland ca. 62 Millionen Bank- und SparkassenCards mit dem GeldKarte-Chip ausgestattet – 70 % aller dafür potenziell in Frage kommender Zahlkarten.[244]

Die GeldKarte ist nicht primär für den Internet-Handel oder für den Einsatz in offenen Netzen konzipiert. Bislang ist die Offline-Welt das Haupteinsatzgebiet der GeldKarte, die sowohl bei Händlerterminals als auch an Automaten eingesetzt werden kann. Die Karte wird durch Finanzinstitute emittiert, eine Alterskennzeichnung auf dem Chip ist problemlos möglich. Somit ist die GeldKarte aus Sicht der mit Altersbeschränkungen belegten Tabakwarenindustrie prädestiniert für den Einsatz an entsprechenden Automaten. Durch verschärfte Jugendschutzgesetze erwarteten sich die GeldKartenbetreiber in den nächsten Jahren allein im Bereich der Zigarettenautomaten 600.000 Umrüstungen.[245]

---

[242] Dabei dringt der Angreifer in die bilaterale Kommunikation der Händler- mit den Kundenseiten ein, manipuliert beispielsweise über die URL Seiten und könnte unter anderem Zugriff auf die PIN und das Passwort erhalten.

[243] Vgl. Europäische Gemeinschaft (2000c).

[244] http://www.geldkarte.de/ww/de/pub/rund_um_die_geldkarte/hintergruende.htm (18.08.2003). Meist ist der Chip kostenfrei für den Kunden, in Einzelfällen wird eine Jahresgebühr um 5 Euro verlangt.

[245] http://www.geldkarte.de/ww/de/pub/die_geldkarte_im_einsatz.htm (18.08.2003).

Die GeldKarte ist mit einem Kartenleser der Sicherheitsklasse 3 (Tastatur, eigenes Display, Transaktionen erfolgen manipulationsgesichert) bereits seit dem Jahr 2000 im Internet bei einigen Händlern einsetzbar. Aufgrund der Hürde für die Nutzer, sich einen solchen Leser anzuschaffen (ab ca. 60 Euro) und zu installieren, ist die Akzeptanz der GeldKarte im Internet (noch) nur bedingt vorhanden. Die Kreditinstitute, die das System betreiben, setzen gleichwohl auf eine kontinuierliche Weiterentwicklung der Umsätze und den Erfolg eingeleiteter Marketingmaßnahmen.[246]

Die Anforderungen des ZKA an die GeldKarte und die Infrastruktur sind sehr hoch gesetzt, beispielsweise ist ein Kartenleser Klasse 3 erforderlich. Dieser garantiert eine hohe Sicherheitsstufe beim Bezahlen im Internet. Dem Kunden wird vor der Bezahlbestätigung beim Bezahlen im Internet neben dem zu zahlenden Betrag die Identität des Geschäftspartners zweifelsfrei angezeigt. Bevor die Bezahlung durchgeführt wird, muss aktiv die angezeigte Summe bestätigt werden. Die hohe Sicherheitsstufe des Kartenlesers schützt den Transaktionsvorgang gegen eine Manipulation des Displays durch Dritte beispielsweise via Viren oder Würmer. Dazu wird bereits auf der Ebene des Kartenlesers die Transaktion verschlüsselt, die dann zusätzlich über eine SSL-Verbindung zum Server geschickt wird.

Im ZKA wurden mit der "Schnittstellenspezifikation für die ZKA-Chipkarte"[247] sowohl für die Offline- als auch für die Online-Zahlung mit der GeldKarte einheitliche Schnittstellen für die Kommunikation aller Beteiligten festgelegt. Die am GeldKarte-System teilnehmenden Geld-Karten-Terminals (physisch oder virtuell) müssen von einer durch den ZKA autorisierten Prüfinstanz (VÖB-ZVD Bank für Zahlungsverkehrsdienstleistungen GmbH, Bonn) in einem Funktionstest einen Konformitätsnachweis mit der Schnittstellenspezifikation des ZKA führen. Dies kann bis hin zu notwendigen Sicherheitevaluierungen führen, die dem ZKA vorgelegt werden müssen und den Nachweis erbringen sollen, dass die "Kriterien für die Bewertung und Konstruktion von chipkartengestützten Zahlungssystemen" eingehalten wurden.[248] Die Betreiber des GeldKarte-Systems sind von der Sicherheit des Systems überzeugt und folgern, „das Falschgeldrisiko entfällt völlig.“[249]

Aus Sicht des Händlers ist das Verfahren hinsichtlich der Zahlungsgarantie zu niedrigen Transaktionskosten (0,3 % des Umsatzes) interessant. Sobald die Transaktion abgeschlossen wurde, ist das Geld unwiderruflich beim Händler (nach entsprechender Verrechnung der Kosten auf Seiten der GeldKarten-Betreiber). Setzen die Händler zugelassene Kartenterminals ein, erhalten sie von den Betreibern der GeldKarte eine Zahlungsgarantie.[250] Das Clearing der über die GeldKarte erfolgten Zahlungen beim Händler erfolgt über Börsenevidenzzentralen, die die Einzeltransaktionen aggregieren. Ein Händlerterminal erhält verschlüsselt die Information, über welche Evidenzzentrale die Beträge verrechnet werden, und auf welches Bankkonto die Gutschrift überwiesen wird. Die eingereichten Umsätze folgen einem einheitlichen Format. Alle Einzeltransaktionen werden bankarbeitstäglich auf Echtheit und Doppeleinreichung geprüft und die Gutschriften und Belastungen der Börsenverrechnungskonten ausgelöst. Die Gutschriften werden am Verrechnungstag über die Gironetze per Überweisung beglichen.

---

[246] Beispielsweise werden gezielt einzelne Städte beworben, aktuelle Maßnahmen vgl. www.geldkarte.de. Auch der (ansonsten bislang wenig publizitätsfreudige) ZKA, der erst seit 2003 über einen eigenen Internetauftritt verfügt, tritt in seinen Veröffentlichungen (nicht nur) im Internet für die GeldKarte ein, vgl. u.a. ZKA (2003b), S. 5 f.

[247] Aktuell gültige Version 3.0 vom 2. April 1998.

[248] Vgl. ZKA (2003a).

[249] ZKA (2003b), S. 6.

[250] Vgl. ZKA (2003b), S. 7.

Die Verlustgefahr des auf der GeldKarte geladenen Betrags kann mit der von Bargeld verglichen werden. Bedingt durch das von den Betreibern vorgegebene Lademaximum von 200 Euro ist dies auch die maximale Schadenshöhe im Verlustfall. Ist die Karte verloren, gibt es keinen Mechanismus für die Sperrung des Schattenkontos und damit der Karte. In den Allgemeinen Geschäftsbedingungen werden die Händler nicht verpflichtet (da es sich um elektronisches Geld, also ein Zahlungsmittel handelt), ihr Guthaben auf den Händlerkarten zeitnah einzulösen. Theoretisch könnte ein Händler noch nach mehr als 30 Jahren auf der Einlösung beharren.[251] Erst nach dieser Einlösung kann jedoch das Schattenkontosaldo aktualisiert werden. Somit stellt der Stand des Schattenkontos nur eine ungefähre aber keine absolute Größe des auf der GeldKarte theoretisch befindlichen Betrags dar. Im Verlustfall, selbst wenn die Karte gesperrt werden könnte, wäre eine Differenz zwischen Schattenkontostand und GeldKarte demnach denkbar und führt zur Verweigerung der Auszahlung an den Karteninhaber.

4.2.6.3 Pay-now-Verfahren

4.2.6.3.1 Nachnahme

Die Nachnahme wird der Vollständigkeit halber bei den Pay-Now-Verfahren aufgeführt. Sie hat mit elektronischem Bezahlen nichts zu tun und ist lediglich für das Bezahlen physischer Güter geeignet, bei denen die Übergabe der Ware und die Bezahlung parallel ablaufen. Der Käufer nimmt dafür in der Regel höhere Gebühren und die Unannehmlichkeit in Kauf, anwesend sein zu müssen, um die Ware in Empfang zu nehmen, oder sie bei der Poststelle abholen zu müssen. Die Sicherheit bezieht der Käufer weniger über die Tatsache, dass er tatsächlich ein Paket in Händen hält, das zudem nicht die gewünschte oder gar defekte Ware enthalten kann. Sicherheit erhält er über die rechtliche Situation bei Mail-order/Telephone-order Geschäften. Demzufolge können Vertragsabschlüsse 14 Tage lang ohne Rücknahmegebühren rückgängig gemacht werden, lediglich bis zu einem bestimmten Warenwert (< 40 Euro) müssen die Portokosten der Rücksendung vom Käufer übernommen werden.

4.2.6.3.2 Online-Lastschrift

Die herkömmliche Lastschrift, geregelt im ZKA-Lastschriftabkommen der Finanzinstitute, bei der nach Vorliegen einer Unterschrift – im Original oder per Fax – der Bevollmächtigte einen autorisierten Betrag einziehen kann, ist im Internet in Varianten zu finden. Ohne Unterschrift des Kontoinhabers wird die Lastschrift von den Kreditinstituten nur bis zu Beträgen von 50 Euro und nicht bei periodischen Zahlungen akzeptiert. Darüber hinaus ist eine Unterschrift zwingend erforderlich. Die rechtliche Lage in Deutschland würde den Einsatz einer qualifizierten digitalen Signatur für die Autorisierung der Lastschrift ermöglichen, allerdings ist die Infrastruktur bislang kaum existent.

Aus Sicherheitssicht ist die Lastschrift bei Internet-Zahlungen doppelt problematisch. Eine gefaxte Unterschrift kann leicht gefälscht werden, erst mit der digitalen Signatur würde dieses Problem gelöst. Zusätzlich riskiert der die Lastschrift Einlösende die berechtigte wie unberechtigte Rückgabe der Lastschrift durch den Zahlungspflichtigen. In letzterem Fall bleibt dem Betroffenen, sollte die Ware bereits ausgeliefert sein, der teure und aufwändige Zivilklageweg. Vorteilhaft ist aus Sicht des Händlers, dass Lastschriften nach den letztes Jahr geänderten AGBs der Banken lediglich bis zu 6 Wochen zurückgenommen werden können.[252]

[251] Vgl. www.geldkarte.de/pub/rund_um_die_geldkarte/faq.htm.
[252] Lastschriftabkommen, Abschnitt III, Nummer 2 (Stand April 2003).

4.2.6.3.3 Mobiles Bezahlen

Mit dem Erfolg des mobilen Telefonierens geht eine Entwicklung erfolgversprechender Geschäftsmodelle rund um die Grunddienstleistung mobile Datenübertragung einher. Grundsätzlich ist das Bezahlen per Handy eine naheliegende Dienstleistung, insbesondere wenn Dienstleistungen mobil übertragen werden und die Telekommunikationsrechnung für die Abrechnung nicht in Frage kommt.

In Deutschland hatte sich als erster national bekannter Anbieter die Firma paybox.net AG mit dem Bezahlsystem paybox 2000 positioniert. Die Deutsche Bank AG war an der Firma beteiligt, aus strategischer Sicht eine erfolgversprechende Konzeption. Gleichwohl reichten mehrere 100.000 angemeldete Nutzer nicht aus, die Transaktionszahlen in eine Höhe zu treiben, die einen kostendeckenden Betrieb ermöglicht hätte – der First-Mover-Advantage wurde wie bereits bei den Systemen eCash und CyberCash als nicht so hoch erachtet, dass sich weitere Investitionen begründen ließen. Anfang 2003 wurde der Betrieb in Deutschland eingestellt, in Österreich wird der Dienst aufrecht erhalten. Da sich im Frühsommer 2003 mit der niederländischen Firma Moxmo N.V. ein Rechtsnachfolger für die Übernahme der Verträge der paybox-Kunden gefunden hat[253] und das grundsätzliche Prinzip von Bedeutung ist, wird im folgenden kurz der Bezahlvorgang der paybox dargestellt.

Die paybox funktioniert nach vorheriger Identitätsfeststellung (und Bonitätsüberprüfung mit Limitvergabe) des Handybesitzers – schriftlich durch Postident-Verfahren. Damit ist die Authentifizierung per Handy technisch und juristisch eindeutig gelöst – die Beweisbarkeit von Transaktionsvorgängen bei Streitfällen gegeben. Dies wird möglich, da neben dem durch eine PIN geschützten Zugang zum Handy zusätzlich für die Bezahltransaktion eine PIN durch den Zahlungssystembetreiber postalisch versandt wird. Das Bezahlen mit dem Handy kann theoretisch an allen Verkaufsstellen geschehen und auch Person-to-Person-Zahlungen umfassen. Voraussetzung ist lediglich eine Handynummer auf Händlerseite oder auf der Seite des privaten Zahlungsempfängers. Im Praxisbetrieb konnte mit der paybox sowohl in Hotels und Taxis als auch im Internet bezahlt werden. Attraktiv war bereits vor in Kraft treten der EU-Überweisungsrichtlinie die Möglichkeit, kostenlos in andere europäische Länder, die an das paybox-System angeschlossen waren, Geld zu überweisen, beispielsweise Österreich oder Spanien.

Der Bezahlvorgang läuft bei einem Bezahlvorgang im Internet durch die Eingabe der Handynummer des payboxfähigen Zahlungspflichtigen in ein vorgegebenes Feld – oder bei Person-to-Person-Zahlungen die Eingabe der Telefonnummer bei einem Telefonat mit dem paybox-Server. Der Händler übergibt die Nummer und den Zahlbetrag an den paybox-Server, der einen automatisierten Anruf an den Zahlungspflichtigen auslöst. Nach Nennung des Betrags und des Händlernamens wird der Zahlungspflichtige aufgefordert, den Zahlbetrag mit seiner paybox-PIN zu bestätigen. Paybox.net AG (nunmehr Moxmo) zieht über eine im Vorfeld schriftlich autorisierte Lastschriftermächtigung den Betrag beim Zahlungspflichtigen für den Händler ein und überweist diesem in vertraglich geregeltem Zeitraum die fällige Summe abzüglich der angefallenen Gebühren.

Das Prinzip ist auch bei anderen Anbietern ähnlich, die technischen Lösungen unterscheiden sich lediglich im Detail. Die Firma Inatec GmbH beispielsweise bietet das derzeit einzige

[253] Auf der moxmo-Homepage (www.moxmo.com/servicedeutschland, Stand September 2003) heißt es: „MOXMO wird den mit Ihnen bestehenden paybox-Vertrag fortführen, die von uns vorsorglich ausgesprochene Kündigung zum 30.06.2003 wird damit hinfällig. MOXMO wird als Ihr neuer Ansprechpartner in alle Pflichten und Rechte eintreten.“ Seit Dezember 2003 ist Moxmo mit dem paybox-Service wieder online für Kunden verfügbar.

operative mobile Bezahlverfahren an, das auch für größere Beträge geeignet ist. Street Cash ist SMS-basiert, die Telefonnummer und der Preis oder Händlername werden per SMS versendet und die Zahlung per SMS bestätigt.

Der Markt für mobiles Bezahlen erscheint hinreichend attraktiv für neue Akteure. Insbesondere versuchen sich in einem zweiten Anlauf internationale Mobilfunkanbieter daran, einen gemeinsamen Standard, Simpay, zu entwickeln und durchzusetzen. Simpay ist ein Gemeinschaftsunternehmen gegründet von Orange, Telefonica Moviles, T-Mobile und Vodafone, offen für weitere Mobilfunkbetreiber.[254] Die Grundidee ist die Abrechung von Micropayments bis Macropayments über eine gemeinsame technische Plattform, die offene Schnittstellen hat und lediglich die Mobilfunkbetreiber zwischen die Anbieter und Konsumenten lässt. Der Verbund großer Mobilfunkbetreiber ermöglicht bei gegenseitiger Anerkennung ein sehr großes Akzeptanznetz und die nötigen Skaleneffekte, die beispielsweise von paybox nicht erreicht werden konnten. Zunächst soll die Initiative auf Europa begrenzt bleiben, im Erfolgsfall global ausgeweitet werden. Der vertragliche Rahmen wird von Simpay gesetzt, so dass supranational das gleiche Regelwerk gilt. Allerdings handelt es sich bei Simpay trotz eigenem Internetauftritt bislang lediglich um eine Willenserklärung. Der Prozess, die verschiedenen Akteure und ihre strategische Positionierung im mCommerce in Einklang zu bringen, wird vermutlich sehr zeitintensiv. Die bisherigen Formulierungen sind sehr offen gehalten, unter anderem, um bestehenden Systemen einzelner Betreiber, beispielsweise m-pay von Vodafone (siehe unten), nicht direkt Konkurrenz zu machen. Stand Sommer 2003 ist weder eine technische Lösung noch ein Starttermin für das operative Geschäft genannt.

In Deutschland auf dem Markt für Micropayments bereits aktiv tätig ist das Bezahlverfahren m-pay der Vodafone D2 GmbH, einem Unternehmen der in Grossbritannien ansässigen Vodafone Group.[255] m-pay ist im Internet über WAP, bei TV-Shops und bei ausgewählten Automaten einsetzbar. Es ist beschränkt auf Personen, die einen D2-Handyvertrag mit Vodafone D2 abgeschlossen haben oder ein Prepaid-Handy dieser Firma besitzen. Der Bezahlvorgang ist je nach Verbindungsaufbau unterschiedlich. Bei Vodafone-WAP-Kaufvorgängen wird der Kunde über die Vodafone-SIM-Karte identifiziert und der entsprechende Betrag über das Vodafone-Kundenkonto oder die Prepaid-Karte abgerechnet. Im Internet muss die D2-Handynummer in das entsprechende Feld eingetragen werden – analog zur paybox – anschließend wird per SMS ein Bezahlcode an diese Nummer verschickt, der 6 Ziffern umfasst und ca. 30 Minuten gültig ist. Dieser Code wird an der vorgesehenen Stelle der Bezahlseite eingegeben und die Zahlung damit autorisiert und abgebucht. Weitere Möglichkeiten sind rein SMS-basierte Transaktionen, beispielsweise zum Bezahlen an Automaten. Vodafone generiert bei der Anfrage SMS an den Automaten eine SMS an den Handybesitzer, die er mit Reply-Funktion kostenfrei bestätigen kann. Der entsprechende Betrag wird vom Konto abgebucht, die Ware freigegeben. Der m-pay-Bezahldienst ist jedem Kunden der Vodafone D2 GmbH ohne Anmeldung zugänglich, kann auf Wunsch jedoch gesperrt werden.

Die jüngste Initiative im Bereich mobilen Bezahlens wurde von der Jamba! AG, einem Gemeinschaftsunternehmen von Debitel, MediaMarkt/Saturn und EP:ElectronicPartner gestartet.[256] Das System handypay funkioniert netzunabhängig und baut auf Technologie der Allpay GmbH auf. Es ermöglicht ab November 2003 derzeit ca. 60 Mio. registrierten Handynutzern von Debitel, T-Mobile, Vodafone und O2 Kleinbeträge (bis 10 Euro) per Handyrechnung oder per Prepaid-Handykarte zu begleichen. Es laufen Verhandlungen mit

[254] Vgl. www.simpay.com (Stand September 2003).
[255] Vgl www.vodafone.de/m-pay (Stand September 2003).
[256] Vgl. www.handypay.de (Stand 20.10.2003).

weiteren Netzbetreibern. Je nach Telefonprovider ist der Bezahlvorgang geringfügig unterschiedlich. Im Kern gibt der Nutzer seine Handynummer auf der Bezahlseite im Internet ein, erhält in der Folge eine SMS, die eine PIN enthält, bei deren Eingabe der gewünschte Inhalt freigeschaltet wird.

Die Sicherheit aller mobilen Bezahlvarianten gilt aus technischer Sicht für die Übertragungswege als sehr hoch. Der Aufwand für das theoretisch denkbare Klonen von SIM-Karten steht in keiner Relation zu dem erzielten Nutzen. Es sind bislang keine Angriffe auf die Transaktionsdaten bekannt. Der Besitz des Handys und zusätzlicher Geheimnisse beispielsweise PIN oder SMS-Code sichert den Bezahlvorgang ab. Die Probleme beim mobilen Bezahlen liegen teilweise bei den dahinterliegenden konventionellen Verfahren, mit denen anschließend die Beträge von den Betreibern eingezogen werden. Hier entscheidet die Qualität der Bonitätsprüfung über die Ausfallwahrscheinlichkeit und -höhe der Zahlungen. Im Rahmen der Aktionen, Kunden zu gewinnen und die Technik aufzubauen, hatte beispielsweise die Paybox.net AG zunächst wegen fehlender Bonitätsprüfungen hohe Rücklastschriftquoten, die aber im laufenden Betrieb auf das übliche Maß zurückgefahren werden konnten. Sicherheitsprobleme können lediglich an der Peripherie auftreten. Beispielsweise gab es bei einem Service-Level der paybox-Dienste für den Händler die Möglichkeit, über eine unverschlüsselte eMail über den Zahlungseingang einer Kundenzahlung informiert zu werden. Dieser Mechanismus konnte dazu genutzt werden, gefälschte Bestätigungsmails zu generieren, die den Händler zur Versendung bestellter Ware veranlassen konnten.[257]

4.2.6.3.4 Online-Überweisung

Bei den Retail-Bezahlverfahren ist das Bezahlen auf Rechnung im Mail-order/Telephone-order Handel physischer Güter nach wie vor an erster Stelle auf der Präferenzskala der Konsumenten.[258] Die anschließende Rechnung kann per autorisiertem Lastschrifteinzug (Unterschrift muss via Fax oder Brief vorliegen) oder per Überweisung beglichen werden.

Bei der Überweisung lassen sich zur Zeit drei Varianten unterscheiden:

1) Die klassische papiergebundene Überweisung bedient sich des Überweisungsträgers, der bei der Bankfiliale abgegeben werden muss,
2) die elektronische Überweisung kann über Online-Banking erfolgen (bei mehr als 20 Millionen Online-Konten in Deutschland immer wahrscheinlicher) oder
3) als direkte Online-Überweisung. Letztere ist als Pay-now-Verfahren einzustufen, da der Händler bei der Rechnungsstellung sofort eine Bestätigung darüber erhält, ob die Überweisung getätigt wurde. Anders als bei einem Lastschrifteinzug ist die einmal getätigte Überweisung rechtsverbindlich, sobald sie das Bankennetz der Kundenbank verlassen hat – der Zeitraum hängt von der eingesetzten Technologie der jeweiligen Bank ab und kann von Sekunden bis zu Tagen reichen.

In Deutschland gibt es Stand Herbst 2003 zwei technologisch unterschiedliche Varianten der Online-Überweisung, die beide im ZKA vorgestellt wurden und genehmigt oder zumindest geduldet werden. Während sich die Firma fun communications GmbH auf eine Lösung konzentriert, die eine direkte Kooperation mit der Bank vorsieht, bei der ein Kunde sein Online-Konto führt, ist die Lösung der Pago eTransactions Services GmbH, eines Gemeinschaftsunternehmens der Deutschen Bank AG und der Beisheim Holding Schweiz AG, ohne

[257] Eigene Erfahrung des Autors mit einem geschädigten Händler im Jahr 2002 bei eBay-Auktion.
[258] Vgl. Leibold (2003).

Kooperation mit der betroffenen Bank möglich – auch wenn diese Kooperation aus Sicht der Pago mittelfristig gewünscht wird.

Bei der Lösung, die fun communications vorsieht, integriert eine Bank die technische Komponente fun HomePay-Modul für die Online-Überweisung in ihr Homebanking-Modul. Die Bank kann dann als Acquirer Händler gewinnen, die als eine Zahlmethode die Online-Überweisung wünschen und mittels weiterer fun-Software an ihr System anschließen. Wird auf Kundenseite die Online-Überweisung gewählt, wird der Kunde direkt über eine SSL-Verbindung zu seiner Bank geleitet. Nach dem üblichen Legitimationsprozess, PIN, HBCI, Signaturkarte, findet er das vertraute Online-Überweisungsformular vor, mit im Unterschied zum „gewöhnlichen" Homebanking bereits vorausgefüllten Feldern. Zur sicheren Zuordnung auf Händlerseite kann der Verwendungszweck vom Kunden nicht mehr verändert werden. Es fehlt die Eingabe einer gültigen TAN. Anschließend erhält der Händler eine Einreichungsbestätigung und kann die Ware sofort versenden. Erste Erfahrungsberichte von Händlern wie dem Reiseveranstalter L'TUR zeigen eine hohe Akzeptanz auf Kundenseite.[259] Mit erweiterten Modulen bietet fun als logischen Schritt eine vollständige „Electronic Bill Presentment and Payment" (EBPP) Lösung an, bei der von der Rechnungsstellung bis zur Bezahlung alle Transaktionen über das Internet laufen.

Eine erweiterte Variante der fun-Online-Überweisung findet sich bei T-Online im Einsatz. T-Online bietet für Kunden die Möglichkeit über die eigene Banking-Plattform ungefähr 800 Banken in Deutschland zu erreichen. Mit dem auf Seite von T-Online bestehenden technologischen Zugriff auf diese Banken, kann das Online-Überweisungsmodul dazwischen geschaltet werden und ohne eigenen Vertrag mit den erreichten Banken deren Online-Banking-Applikation verwendet werden. Auf Kundenseite stellt sich der Bezahlvorgang analog zu dem oben beschriebenen dar.

Ein technisch unterschiedliches Verfahren verwendet die von Pago eingesetzte Lösung, die ursprünglich in einem Joint Venture der Deutschen Bank AG und der Unternehmensberatung Accenture, beim Unternehmen Stackbox, entwickelt wurde und nach der Auflösung des Unternehmens von Pago weiterentwickelt und vertrieben wird. Mit dem Verfahren können circa 2.000 Kreditinstitute erreicht werden und deren Kunden die Online-Überweisung angeboten werden.[260] Anbieter des Verfahrens gegenüber dem Händler ist die e-Prompt Germany Commercial Services GmbH, ein weiteres Tochterunternehmen der Beisheim Holding Schweiz AG. Der Bezahl-vorgang verläuft auf Kundenseite mittels eines temporären Java-Applets, das auf den Rechner des Kunden geladen wird. Dort muss die Bank- und Kontoverbindung eingegeben werden und mit der PIN freigegeben werden. Anschließend wird von dem Applet – ohne die PIN auf einem Pago-Server zu verwenden – direkt eine verschlüsselte SSL-Verbindung zur entsprechenden Bank aufgebaut, und ein vorausgefülltes Überweisungsformular generiert. In dieses Formular kann dann eine gültige TAN eingegeben werden, die den Bezahlvorgang formal abschließt. Technisch basiert die Lösung der Firma Pago darin, die bestehenden Online-Banking-Masken der entsprechenden Banken auf ihre Eingabefelder zu untersuchen, und die vom Kunden eingegebenen Daten mit denen des Händlers zu verbinden, um anschließend die Felder im Online-Banking-Formular der Bank vorauszufüllen und dem Kunden so zu präsentieren, als hätte er selbst diese Verbindung eröffnet. Bei erfolgreicher Einreichung der Überweisung erhält der Kunde eine Bestätigung, der Händler, sofern er über e-Prompt das Kommissionsverfahren nutzt, eine (allerdings gebührenpflichtige) Zahlungsgarantie. Rechtlich ist diese möglich durch die Gestaltung der

[259] Vgl. o.V. (2003).
[260] Vgl. www.pago.de/index.php?id=113 (09.09.2003).

Allgemeinen Verkaufsbedingungen von e-Prompt.[261] Demnach tritt die e-Prompt GmbH als Verkaufkommissionärin im Sinne der §§ 383 ff. HGB auf und verkauft Waren und Dienstleistungen auf Kommissionsbasis für den Betreiber eines eShops. Durch diese Lösung wird ein Konsument Kunde nicht des Online-Shops sondern der e-Prompt GmbH. Der Shopbetreiber wird zum Kommittenten des Unternehmens. Gleichwohl hat der Kunde die gleichen Rechte gegenüber dem Shopbetreiber, die er auch bei direktem Abschluß des Vertrags mit dem Shop hätte, und die vom Fernabsatzgesetz zugestanden werden (Rücktritt vom Kauf binnen 14 Tagen, kostenlose Warenrücksendung bei Beträgen über 40 Euro etc.).

Die Sicherheit des Händlers bei ordnungsgemäßer Lieferung der Ware sein Geld zu erhalten, ist bei der Online-Überweisung sehr hoch und im Fall der Zahlungsgarantie ohnehin gegeben. Zusätzlich steht zu vermuten, dass Personen, die auf betrügerische Handlungen aus sind, das rechtlich schwächere Konstrukt der Lastschrift ausnutzen und auf Angriffe bei der Online-Überweisung verzichten. Aus Kundensicht besteht lediglich die Gefahr, dass der Händler nicht die gewünschte oder gar keine Ware liefert. Ist die Überweisung dann bereits ausgeführt, bleibt nur der umständliche Zivilklageweg. Somit hängt die Sicherheit des Kunden beim Bezahlvorgang wesentlich von der Auswahl der Händler durch den Zahlungsanbieter der Online-Überweisung ab.

Die Sicherheit der verschlüsselten Vorgänge bei der Online-Überweisung ist letzlich so hoch wie das eingesetzte Online-Banking-Verfahren es zulässt. Die Verwendung einer TAN für jede Transaktion reduziert Angriffsverfahren gegen Kunden erheblich. Es bleibt lediglich ein Szenario, in dem ein Angreifer, eine gefälschte Seite generiert, mit der ein Kunde neben der Bank- und Kontoverbindung zur Eingabe von PIN und TAN aufgefordert wird. Hat der Angreifer diese Information, kann er zumindest eine missbräuchliche Transaktion ausführen und hat anschließend über die PIN Kontoeinsicht. Diese Problematik ist bei der Online-Überweisung, die durch einen Shop initiiert wird, unter Umständen größer als bei der bisher üblichen Überweisung im Online-Bankingverfahren. Dessen Umgebung (Erscheinungsbild, Anzahl notwendiger Schritte etc.) ist den Kunden mittlerweile vertraut, eine Voraussetzung, die für einzelne Shops mit verschiedenen Webauftritten nur bedingt gilt.

4.2.6.3.5 Bezahlen per eMail

Der Erfolg von PayPal, einem Bezahlsystem per eMail, basiert einerseits auf dem Erfolg von eBay-Auktionen und andererseits auf dem Mangel an geeigneten P2P-Bezahlverfahren in den USA. Zusätzlicher Erfolgsfaktor war eine konsequente Ausrichtung auf die Nutzer des Verfahrens und ihre Bedürfnisse – im Gegensatz zu anderen Verfahren wie eCash, die stark technologiegetrieben waren. Hinzu kamen intensive Werbeaufwendungen – anfänglich bekamen Neukunden und Werber bis zu 10 US-$.[262] Auch vier Jahre nach der Gründung setzt PayPal, seit 2002 in Besitz der eBay Inc., auf Anreize. Mittlerweile werden bei bestimmten Käufen über eBay PayPal-Bonuspunkte vergeben. PayPal ist Stand Sommer 2003 in 38 Ländern operativ tätig, hat 30 Mio. Nutzerkonten (gegenüber 20 Mio. im Oktober 2002) und 42.000 Shops, die das Bezahlsystem akzeptieren.[263]

---

[261] Vgl. www.e-prompt.de/epromptagb.pdf.

[262] Mittlerweile werden 5 US-$ für Neukunden gutgeschrieben, die mindestens 250 US-$ auf ihr Konto eingezahlt haben und sich für den Money Market Fonds angemeldet haben, der zinsbringend die PayPal-Guthaben anlegt. Erfolgt die Anmeldung zum Fonds nicht, fallen die Einnahmen, die PayPal kollektiv in solchen Fonds anlegt, laut AGBs an PayPal. Ein einen Neukunden empfehlender PayPal-Kunde erhält ebenfalls 5 US-$ für eine erfolgreiche Neukundenvermittlung.

[263] www.paypal.com.

Grundsätzlich kann mit PayPal Geld per eMail gesendet, eingefordert und entgegengenommen werden.[264] Zur Nutzung des PayPal-Dienstes ist eine Registrierung notwendig, die online möglich ist und keinen postalischen Zusatzschriftwechsel erfordert. Allerdings ist die Hinterlegung einer Kreditkartennummer nötig, um einen vollen Kontozugang zu PayPal zu erhalten. Drei Kontotypen können unterschieden werden – Personal Account, Premier Account und Business Account – die sich in Gebührengestaltung und Servicelevel unterscheiden. Der Zugang zu den PayPal-Diensten wird per Login (eMail-Adresse und Passwort) auf den Internetseiten von PayPal möglich. Es wird eine gesicherte SSL-Verbindung aufgebaut. Dort kann dann Geld durch Eingabe einer Empfänger-eMail-Adresse verschickt werden, oder bei Empfang von Geld, der Betrag akzeptiert werden (kann auch automatisiert werden). Empfängt ein PayPal-Teilnehmer Geld erfährt er dies durch eine eMail von PayPal: „You've Got Cash!". Die Anforderung von Geld, analog zur Rechnungsstellung, erfolgt nach dem Login mit Angabe des Grundes für die Anforderung, Betrag etc. Der Aufgeforderte erhält anschließend von PayPal eine eMail mit einem Link auf die PayPal-Seite. Durch Einloggen und Bestätigen der entsprechenden Meldung kann die Rechnung bezahlt werden. Wie bei der Online-Überweisung lässt sich das System somit einfach in EBPP-Lösungen integrieren. PayPal-Konten sind somit ein in sich geschlossenes Clearing-System. Die Außenbezüge werden über Kreditkarten- oder auch Girokonten hergestellt, auf die empfangenes Geld (gegen Gebühr) gezahlt werden kann, oder ein PayPal-Konto aufgeladen werden kann. PayPal hat in den USA mittlerweile auch den Schritt in die physische Bezahlwelt vollzogen und emittiert eine Debitkarte, die auf das PayPal-Konto zugreift und Bargeldabhebungen an Geldautomaten ermöglicht.

PayPal Inc. fällt in den USA zwar in einigen Staaten unter die Finanzaufsicht, der Dienst wird jedoch nicht als Einlagengeschäft verstanden. Somit fällt PayPal nicht unter den Zwang, eine Einlagensicherung zu betreiben, gibt jedoch auf seiner Webseite an, über 50 Mio. US-$ an eingezahltem Eigenkapital und Barmitteln zu verfügen. Für Verkäufer und Käufer hat PayPal mittlerweile unterschiedliche Sicherungsmodelle im Angebot.[265] Beispielsweise können Käufer eine Zahlungsgarantie kaufen, die ihnen im Schadensfall diesen ersetzt. Verkäufer können als verifizierte Verkäufer gelistet werden, deren Legitimität PayPal überpüft hat. Verkäufer erhalten zwei Seiten mit Hinweisen (Seller Protection Policy), welche Punkte sie bei Verkäufen beachten sollten, um betrügerische Käufer zu vermeiden, unter anderem wird empfohlen, Waren nur an eine bestätigte Adresse zu senden. Diese Adresse stimmt mit der Adresse überein, die bei der Kreditkartenorganisation zur Versendung der Abrechnung angegeben wurde.

In Europa hat sich ein weiterer Anbieter eines eMail-basierten Bezahlsystems etabliert, die Firma Moneybookers Ltd., eine Tochterfirma der in London ansässigen Beteiligungsgesellschaft Gatcombe Park Ventures Limited – einem Nichtbanken-Unternehmen. Moneybookers Ltd. ist die erste Nichtbank, die in Europa den Status eines eGeld-Instituts gemäß EU-Richtlinie erhalten hat.[266] Moneybookers fällt unter englisches Recht und unterliegt der Aufsicht der Financial Services Authority (FSA) in Großbritannien. Damit steht das Unternehmen in der Pflicht zu jedem Zeitpunkt genügend liquide Mittel vorzuhalten, um das umlaufende eGeld auszahlen zu können. Die Vorgaben zur Bekämpfung der Geldwäsche müssen eingehalten werden, unter anderem bedeutet dies, dass mit Moneybookers im Quartal keine höheren Umsätze als 15.000 Euro getätigt werden dürfen.

[264] Vgl. www.paypal.com und Nitschke (2002).
[265] Vgl. www.paypal.com.
[266] Vgl. Europäische Gemeinschaften (2000c).

Bei der ersten Zahlung oder dem Empfang von Geld mit Moneybookers ist wie bei PayPal eine Registrierung notwendig, anschließend kann, ein Guthaben vorausgesetzt, mit eMail-Adresse und Passwort bezahlt werden. Im Gegensatz zu PayPal werden laut AGBs Absatz 3.4. die Guthaben nicht verzinst, dafür sind die Gebühren für Transaktionen niedriger als bei PayPal. Die Sicherheit der Systemkunden wird über verschlüsselte SSL-Verbindungen garantiert. Für die Kombination von Passwort und eMail-Adresse, mit der Transaktionen bestätigt werden, respektive deren Einsatz, haftet laut AGB Absatz 4.2. auch im Betrugsfall der Kunde. In Absatz 8 der AGB werden ferner alle Schadensfälle durch betrügerisches Handeln aber auch durch Datenübertragungsfehler als nicht schadensersatzpflichtig durch Moneybookers vereinbart. Rechtlich wird der Geldtransfer bei Moneybookers der deutschen Überweisung gleichgestellt. In Absatz 9.3. wird festgestellt:[267] „Ein von Moneybookers durchgeführter Geldtransfer kann nicht mehr annulliert oder in irgendeiner Form geändert oder rückgängig gemacht werden."

Ein Großteil der Bezahltransaktionen laufen in den internen Netzen der Betreiber. Gleichwohl handelt es sich bei den eMail-Bezahlverfahren um klassische Zugangsprodukte zu den etablierten Zahlungsnetzen, Girokonten und Kreditkartennetz.

4.2.6.4 Pay-later-Verfahren

4.2.6.4.1 Kreditkarte

Die Kreditkarte ist weltweit das gebräuchlichste Zahlungsmittel im Internet. Der Grund liegt neben der Einfachheit des Bezahlvorgangs (Kreditkartennummer, Gültigkeitszeitraum und Namen eingeben) in der Größe der Kreditkartennetzwerke. Die beiden größten Kreditkartennetze besitzen Visa International mit VisaNet und MasterCard International mit BankNet.[268] Visa gibt an, mehr als 50 % aller weltweit getätigten eCommerce-Transaktionen würden über die eigene Organisation laufen.[269]

Der Bezahlvorgang läuft bei Kreditkartenzahlungen herkömmlicher Art, das heißt ohne Berücksichtigung neuer Sicherungsverfahren, über (meist) SSL-verschlüsselte Verbindungen. Kunden, die Waren erwerben, geben auf der Shopseite ihre Kreditkartennummer, Name, Adresse und eventuell noch sicherheitserhöhend (da die reine Kreditkartennummer, die auf Belegen erscheint, nicht ausreicht) CVV2[270] oder CVC2[271] ein. Die zusätzlichen Prüfcodes vermitteln allerdings nur ein partielles Sicherheitsgefühl. Zwar sinkt durch die Auflagen, die unter anderem die Händler von den Acquirerbanken bezüglich der (verbotenen) Speicherung dieser Prüfziffern erhalten, die Wahrscheinlichkeit des elektronischen Kartennummernraubs. Organisierte Kartenkriminalität verweist jedoch auf Netzwerke, die mit Betrügern am Point-of-Sale zusammenarbeiten. Bei der Aktzeptanz einer physisch vorliegenden Kreditkarte ist es für Betrüger ein Leichtes, zumal wenn die Karte aus der Hand gegeben wurde, die Prüfziffern zusätzlich zur Kartennummer zu erhalten. Dieses Problem wird den Kreditkartenbesitzern von den kartenausgebenden Banken nicht kommuniziert. Eine einfache Lösung wäre beispielswei-

[267] Moneybookers (2003b).
[268] Zur Organisation der Kreditkartenorganisation siehe 4.3.1.2.
[269] http://corporate.visa.com (10.09.2003). Unter eCommerce wird im folgenden elektronischer Handel verstanden, der im Internet stattfindet und in der Regel auf Business-to-Consumer beschränkt ist. Zahlverfahren im Business-to-Business-Segment unterliegen grundsätzlich anderen Regeln, da vielfach gewachsene Lieferbeziehungen existieren.
[270] Card Verification Value, verwendet von Visa. Es handelt sich um einen dreistelligen Prüfcode, der auf der Rückseite der Visa-Karte aufgedruckt ist und nicht auf Belegen abgedruckt wird.
[271] Card Validation Code, verwendet von MasterCard. Ein dreistelliger Prüfcode, der auf der Rückseite der MasterCard aufgedruckt ist und nicht auf Belegen abgedruckt ist.

se das Unkenntlichmachen der CVV2/CVC2-Codes auf der Karte und das auswendige Merken dieser Nummer oder deren Notiz an anderer Stelle. Auf Händlerseite werden die Daten bei der Bank (Acquirer), bei der der Händler den Kreditkartenvertrag unterzeichnet hat, eingereicht, überprüft, und die Transaktion in die Kreditkartennetze geleitet. Gutschriften und Lastschriften, die aus den Kartentransaktionen resultieren, laufen nach dem Clearing durch die Kreditkartengesellschaft über die Massenzahlungssysteme der Bankenwelt zum Settlement.

Schwierigkeiten mit Betrug bei Kreditkartenzahlungen und der resultierenden negativen Öffentlichkeitswirkung, verbunden mit dem Anspruch der Kreditkartenunternehmen sichere Systeme anzubieten, haben in den letzten Jahren zu verschiedenen Sicherheitskonzepten geführt, darunter die bedeutendsten und teils aufeinander aufbauenden Secure Electronic Transaction (SET), EMV-Chip (benannt nach den Anfangsbuchstaben der Entwicklerfirmen Europay, Mastercard (beide mittlerweile fusioniert) und Visa), „Verified by Visa“ und „SecureCode“ von MasterCard.

Der Grundgedanke bei allen innovativen Sicherungskonzepten ist der gleiche: Ein Käufer, der eine Zahlkarte einsetzt, braucht ein Geheimnis, mit dessen Hilfe er sich zweifelsfrei bei Transaktionen in offenen Netzen authentifizieren kann. Die dazu notwendigen Daten müssen verschlüsselt kommuniziert werden. Auch die neueren Verfahren basieren auf den Grundsatzarbeiten von SET.

SET wurde von 1996 bis 1998 von der Kreditkartenindustrie gemeinsam auf der Grundlage der Verwendung digitaler Signaturen entwickelt. Bei diesem Verfahren installiert der Karteninhaber eine Software auf seinem Rechner (SET Wallet), die beim Einkaufsvorgang aufgerufen wird. Der Zugang zur Wallet kann beispielsweise per PIN geregelt werden. Die SET-Software des Einkäufers kommuniziert anschließend mit der SET-Software des Händlers (SET Händler Wallet). Daraufhin wird über diese Software und ein SET Gateway beim Acquirer des Händlers via Kreditkartennetz (VisaNet oder BankNet) eine Autorisierungsanfrage bei der kartenausgebenden Bank (Issuer) des Kunden gestellt. Die Antwort geht den gleichen Weg retour. Das Besondere an der SET-Vorgehensweise ist neben der verschlüsselten Kommunikation die eindeutige Identifikation der beteiligten Parteien über digital signierte SET-Zertifikate – und damit Haftung für beide Parteien und fehlende Rücklastschriftmöglichkeit für den Kunden[272]. Zusätzlich lassen sich Warenkorbinformationen und Zahlbeträge in einer einmal angestoßenen Transaktion nicht mehr verändern.

Schürer kommt in seiner Analyse zu dem Schluss, dass neben der Unwilligkeit der Konsumenten Software auf ihrem Rechner zu installieren, die hohen Kosten einer Public Key Infrastructure (PKI) unterschätzt wurden und ebenso der hohe Integrationsaufwand auf Händlerseite. Hinzu kam eine generelle Verweigerung der US-Märkte zum Thema SET. In der Folge betrachtet Schürer SET bereits Ende 2001 als in Europa gescheitert.[273] Alleine die Einführung so genannter Server Wallets, die auf Kundenseite passwortgeschützt erreicht werden können, kann diese Problematik nicht entschärfen. Neue Verfahren wurden daraufhin entwickelt.

Auf Seiten von Visa wurde 3D-Secure, nunmehr vermarktet unter dem Namen „Verified by Visa“, entwickelt. MasterCard entwickelte „SecureCode“. Basis ist für beide Verfahren das Three-Domain-Konzept (3D), bei dem die Issuer-Domain, eine Interoperability-Domain und eine Acquirer-Domain unterschieden werden. In der Issuer-Domain wird von der Kundenbank

[272] Zumindest das übliche Argument „War ich nicht!“ verliert seine juristische Gültigkeit.
[273] Vgl. Schürer (2002), S. 217ff.

die Identität des Karteninhabers über ein frei wählbares Verfahren (PIN, Chipkarte etc.) festgestellt – dazu muss der Kunde einen Registrierungs/Anmeldungsprozess bei seiner kartenausgebenden Bank durchlaufen haben. Die Interoperability-Domain sichert die Kommunikation zwischen der kartenausgebenden Bank und der Händlerbank. Die Acquirer-Domain dient der gesicherten Kommunikation und Zahlungsabwicklung von Händler und Acquirer – die dazu auch eine gesonderte Vertragsbeziehung eingehen.

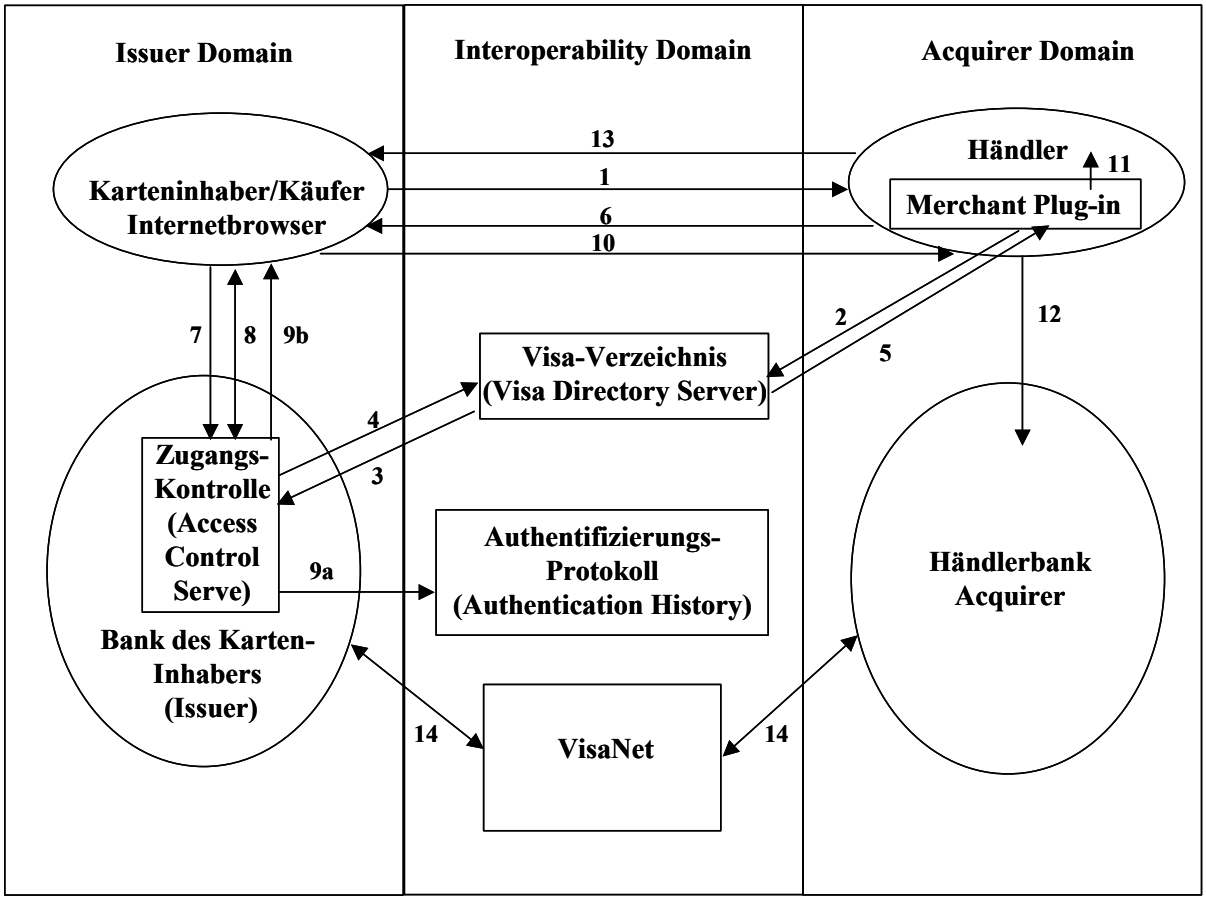

Abbildung 14: Bezahlvorgang mit Kreditkarte bei Visa 3D-Secure (Verified by Visa)[274]

Der Bezahlvorgang mit 3D-Secure läuft ab, wie in Abbildung 14 skizziert:[275] Im ersten Schritt (1) geht der Käufer mit der Ware zur virtuellen Kasse und gibt seine Kreditkartennummer an. Anschließend wird (2) durch ein Plug-in auf der Händlerseite, das dieser zuvor in seine Bezahlsoftware integriert haben muss, das Visa-Kartenverzeichnis über das Internet angefragt. Es wird überprüft, ob die Nummer valide und bei 3D-Secure angemeldet ist. Im positiven Fall wird der Zugangskontroll-Server der Kundenbank angefragt (3)und schickt bei positiver Überprüfung diese Information über das Visa-Verzeichnis (4) zum Plug-in des Händlers zurück (5). Danach wird dem Karteninhaber über seinen Browser (6) vom Plug-in eine Authentifizierungsanfrage (Payer Authentication Request) (7) über den Kundenbank-Server weitergeleitet und gestellt (Passworteingabe, HBCI etc.) (8). Die Authentifizierungs-nachricht wird vom Zugangsserver der Issuer-Bank verschlüsselt. Die verifizierte Nachricht wird in (9a) einerseits an den Visa Authentification History Server zur Speicherung geschickt (Beweissicherung), andererseits an den Browser des Kunden (9b) zurück zum Plug-in des Händlers (10) gesendet. Das Plug-in (11) prüft die verschlüsselte Nachricht auf Korrektheit

[274] In enger Anlehnung an Visa (2003), S. 23.
[275] Vgl. Visa (2003), S. 24 f.

und bestätigt dem Händler den Vorgang, der dann in (12) den Bezahlvorgang im Fall einer positiven Nachricht mit seiner Händlerbank fortsetzen kann, und den Warenkorb (13) virtuell oder physisch ausliefern kann. Das Clearing der Zahlung geschieht anschließend (14) im VisaNet der Vertragsparteien. Im Vertragsregelwerk zwischen Visa und Händler wird dem Händler bereits dann eine Zahlungsgarantie gegeben, wenn er seine Systeme auf 3D-Secure umrüstet – ohne dass der Käufer bei 3D-Secure angemeldet sein muss.

Eine Bezahltransaktion mit MasterCard SecureCode basiert auf der UCAF/SPA-Technologie (Universal Cardholder Authentification Field (html-Codezeilen, die der Händler einfach auf seiner Seite implementieren kann und muss, und die als „hidden fields" nicht für den Surfer sichtbar werden[276])/Secure Payment Application). UCAF bietet einen Interoperabilitätsstandard, der im 3-Domain-Modell die Authentifizierungsvorgänge zwischen Händler, Kunde und Banken sicherstellt und eine Zeichenfolge mit maximal 32 Stellen verschlüsselt durch offene Netze transportiert. SPA stellt über eine 32-stellige Zahl (Accountholder Authentication Value (AAV)), die alle notwendigen Transaktionsdaten beinhaltet und die UCAF-Infrastruktur nutzt, nachweisbar sicher, dass eine Bezahlung von der registrierten Person getätigt wurde. Damit kann das Chargeback-Risiko für Händler und Bank gesenkt werden.

Der Vorgang ist weitgehend analog zu einer Visa-Zahlung. Für den Bezahlvorgang auf der Bezahlseite des Händlers trägt zunächst der Kunde seine Kartendaten (Kreditkartennummer) ein. [277] Vom Händler, der in seine Bezahl-Software ein Merchant-Plug-in (MPI) einbauen muss[278], wird eine Verbindung zum MasterCard-Router aufgebaut, der die Daten an die Issuer-Bank weiterreicht. Beim Kunden wird ein Pop-up-Fenster geöffnet, in dem er gegenüber seiner Bank die SecureCode-Anmeldedaten eingibt. Die Issuer-Bank schickt die Authentisierungsdaten im Erfolgsfall über den Browser des Kunden an den Händler. Sie werden auf dessen Internetseite in das (unsichtbare) UCAF eingetragen. Die vollständigen Daten der Transaktion werden vom Händler an die Acquirer-Bank, die für MasterCard SecureCode ebenso angemeldet und registriert sein muss wie der Händler, weitergereicht. Nach positiver Überprüfung der signierten Nachrichten und des Autorisierungscodes wird die Transaktion autorisiert. Die Ware kann ausgeliefert werden. Die Verrechnung zwischen den Banken findet über MasterCard's BankNet statt.

Gab es zunächst zwischen 3D-Secure und SecureCode den Unterschied, dass MasterCard-Kunden ein kleines Softwarepaket (Applet) herunterladen mussten, um SPA zu unterstützen, während Visa-Kunden ohne Installationsaufwand einkaufen konnten[279], ist diese Hürde mittlerweile genommen. Im deutschsprachigen Raum ist bei MasterCard nur noch von einem Pop-up-Fenster im Browser des Kunden die Rede, eigene Softwareinstallationen erübrigen sich[280] – MasterCard baut für diese Lösung wie Visa auf die 3D-Technologie auf.[281] Für die Durchsetzung des Verfahrens sicherlich eine der wichtigsten Änderungen gegenüber den ursprünglich angedachten Technologien. Ein Unterschied besteht in dem Autorisierungsprozess gegenüber der Bank. Während Visa-Kunden ihre ursprünglichen Legitimationsdaten aus dem Online-Banking verwenden können (es besteht auch die Möglichkeit einer separaten

[276] Das Verstecken des Codes hat dabei keine Sicherheitsfunktion, sondern dient lediglich der Übersichtlichkeit der Seite, die der Händler dem Kunden präsentiert.
[277] Vgl. Siegert (2002), MasterCard (2003).
[278] Das MPI übernimmt die Authentifizierungs- und Zahlungsvorgänge mit Bank/Servern und Kunde im Hintergrund. Für die Verschlüsselungsvorgänge muss der Händler zusätzlich ein SSL-Client-Zertifikat und das MasterCard-Root-Zertifikat implementieren, vgl. www.acceptance.de/sicherheit/mastercard/funktion/index.jsp (09.09.2003).
[279] Vgl. Schürer (2002), S. 219 ff.
[280] Vgl. www.mastercard-securecode.ch/sc_index/sc_faq.htm. (09.09.2003).
[281] Vgl. https://ipayment.de/frameset.php4?frame=news (09.07.2003), MasterCard (2003), Abschnitt 3-1 ff.

Passwortvergabe) wird bei MasterCard SecureCode bei der notwendigen Anmeldung der Kunde aufgefordert, seinen SecureCode mittels Anmeldefenster selbst zu erzeugen.[282] Der SecureCode besteht aus 6-10 Zeichen mit mindestens einem Buchstaben und einer Zahl, Leerzeichen sind nicht erlaubt). Dieser SecureCode ist für die Bezahlung mit Kreditkarte per MasterCard SecureCode zwingend für jede Transaktion notwendig. In einem weiteren Schritt sollen in Zukunft auch Maestro-Debitkartenzahlungen mit dem gleichen Verfahren im Internet möglich werden.

Die Problematik des Kreditkartenbetrugs wurde in den letzten Jahren zwar zunehmend durch den eCommerce öffentlich, der Betrug mit Karten am Point-of-Sale (POS) hatte jedoch parallel zugenommen. Die Fälschungssicherheit der Magnetstreifen war insbesondere für die organisierte Kriminalität nicht gewährleistet.[283] 52 % der Kreditkartenbetrügereien in Deutschland sind auf Kartenfälschung zurückzuführen. Dabei resultieren 95,5 % der betrügerischen Transaktionen aus länderübergreifendem Einsatz der Karte.[284] In der Folge wurde von den großen Kreditkartenorganisationen Europay (mittlerweile MasterCard), MasterCard und Visa für die Kreditkartenzahlung per Chip der EMV-Chip entwickelt und spezifiziert[285] und mittlerweile auch von anderen Kreditkartenorganisationen adaptiert. Neben Kreditkartenzahlungen sollen auch Maestro (Nachfolger der ec-Karte) als Debitkarte und Visa-Electron[286] über EMV abgewickelt werden. Es gibt derzeit noch zwei gültige EMV-Spezifikationen (EMV 96, Version 3.1.1 und EMV 2000, Version 4.0), die noch bis 2004 parallel laufen können. Die Spezifikation regelt die sichere Kommunikation zwischen Chipkarte und Terminal und umfasst die Beschreibung der elektromechanischen Eigenschaften der Karte, die Schnittstellen und Protokolle, die Kommandozeilen, den Prozessablauf der Kommunikation und die verwendbaren Terminals. Ein Vorteil der Smartcards ist neben der höheren Fälschungssicherheit die Möglichkeit, Zusatzanwendungen, beispielsweise Bonuspunkte, auf der Kreditkarte zu implementieren[287] – analog zu den Modellen bei der GeldKarte. Der Migrationsplan sieht vor, dass in Europa bis 01.01.2005 alle Terminals EMV-fähig sein müssen, ab diesem Zeitpunkt geht die Haftung für Kreditkartenzahlungen von der Issuer-Bank auf die Geschäftsbank des Terminalinhabers (Acquirer) über.

Die Technologie der Chipkarte, insbesondere die sichere Authentifikation, bietet sich für Bezahlsysteme im Internet an. Allerdings um den Preis der Installation eines Chipkartenlesegeräts, mit den von der GeldKarte bekannten Problemen auf Kundenseite. Auf der CeBIT 2002 wurde erstmals von der EURO Kartensysteme, Europay International, SRC GmbH und VÖB-ZVD Bank für Zahlungsverkehrsdienstleistungen eine Lösung zum Bezahlen über den EMV-Chip im Internet vorgestellt.[288] Der Vorteil des Systems liegt gegenüber der GeldKartenzahlung im Internet in der demnächst international gebräuchlichen EMV-Architektur. Dabei bedient sich der EMV-Chip bei einer so genannten e-smart-Transaktion der von MasterCard aufgebauten UCAF-Infrastruktur im Internet. So kann der Karteninhaber mittels Chip authentifiziert werden, die Transaktionsdaten werden mittels Chip in ein „Transaktionskryptogramm“ umgerechnet, das über den Kartenleser des Kunden an die Händlerbezahlsoftware weitergeleitet wird. Auf Händlerseite werden mithilfe der UCAF-Technologie die Transaktionsdaten über die Acquirer-Bank an die Issuer-Bank weitergeleitet und von dort die Zahlung autorisiert. Das System umgeht dabei die bei SecureCode und 3D-Secure noch

[282] Vgl. MasterCard (2003), S. 3-10.
[283] Vgl. Preuß (2002).
[284] EPS (2003).
[285] Vgl. Siegert (2002).
[286] Eine Prepaid-Debitkarte von Visa.
[287] Vgl. o.V. (2002b), S. 1 f.
[288] Vgl. Siegert (2002) und Smart-e (2002).

notwendigen Wallet-Server – allerdings um den Preis eines Kartenlesegerätes, das auf Kundenseite erworben und installiert werden muss.

Die neu aufgesetzten Sicherheitskonzepte bei Kreditkartenzahlungen gehen einigen Anbietern nicht weit genug. Die Certification Authority, zentrale Instanz bei der Zertifikatserstellung, und Dienstleister im Internet, die Firma VeriSign bietet Händlern seit Mitte 2003 die Möglichkeit, mithilfe des so genannten Fraud Protection Service weltweit die Kombination aus Kartennummer, Name und Wohnort des Besitzers online zu überprüfen.[289] Allerdings beruht die Annahme von VeriSign, dass Händler im Internet durch Betrug bei Kreditkartenzahlungen momentan rund sieben Prozent ihres Umsatzes verlieren, auf den bislang üblichen Verfahren der Kreditkartenzahlung im Internet. Es kann erwartet werden, dass die flächendeckende Verbreitung der neuen Technologien „Verified by Visa“ und „SecureCode“ die Betrugsrate drastisch senken wird. Allerdings umfasst der Service von VeriSign noch andere Dienste, die grundlegende Sicherheitsprobleme bei Händlern abstellen sollen, unter anderem eine Sicherheitsüberprüfung der Shops durch IT-Security-Fachleute.

4.2.6.4.2 Billingverfahren

Für die Abrechnung kleinerer Beträge gibt es spätestens seit der Einführung der Telefonrechnung die Möglichkeit, diese Beträge aufzusummieren und in der Regel am Ende eines Monats einzufordern, meist per Lastschrifteinzug aber auch per Rechnungsstellung. Mitte der neunziger Jahre gab es zunächst die Vorstellung, diese Systeme könnten durch technische Lösungen (beispielsweise Millicent von IBM) obsolet werden. In der Internet-Realität haben sich sowohl Prepaid-Micropaymentsysteme als auch Billingverfahren[290] durchgesetzt.

In Deutschland gibt es zwei große Akteure im Markt der Abrechnungsdienstleistungen für digitale Güter, die Deutsche Telekom AG mit dem Produkt T-Pay, einer Zahlungssystemplattform, bei der über Telefonrechnung, Prepaid-Karte oder Kreditkarte bezahlt werden kann, und die Firstgate Internet AG, mit dem Produkt FIRSTGATE click & buy™. Die Dienstleistungen der beiden Anbieter lassen sich in zwei Bereiche unterteilen. Zum einen bieten sie den Vertragsunternehmen (Händlern) eine Tarifierungsmöglichkeit. Zum anderen rechnen beide Anbieter im Rahmen eines Factoring-Vertrags mit ihren Vertragspartnern ab.[291] Dabei handelt es sich um offenes Factoring, der Schuldner (Kunde) wird über die Abtretung der Forderung an den Zahlungssystemanbieter informiert. Allerdings übernehmen die Anbieter keine Delkredererisiken (Kreditrisiken), daher handelt es sich um unechtes Factoring.

Die eigentliche Leistung der Verfahren liegt neben der technisch aufwändigen Abrechnungsplattform in der kosteneffizienten Addition von Kleinbeträgen bei den einkaufenden Kunden und der dadurch möglichen monatlichen Abrechnung. Der Vorteil für die Kunden liegt in der Vielfalt der Angebote, die nach erfolgreicher Registrierung mittels einfacher Autorisierung per Passwort bezahlt werden können – ohne anschließend bei jedem einzelnen Anbieter Kleinbeträge begleichen zu müssen. Formal handelt es sich bei den Billingverfahren um Zugangsprodukte zum herkömmlichen Zahlungsverkehr. Bei Firstgate wird die aufsummierte

[289] Vgl. http://www.verisign.com/products/payflow/fraud/protection.html (09.09.2003).
[290] Der häufig verwendete Begriff Inkassoverfahren ist in der Regel unzutreffend. Inkassounternehmen werden im Allgemeinen eingesetzt, um notleidende Forderungen einzutreiben.
[291] Bei T-Pay gilt dies nur für den Bereich Prepaid-Karten und Abrechnung über Telefonrechnung. Für die Kreditkartenzahlung übernimmt T-Pay die technische Anbindung, der Kartenakzeptanzvertrag wird über eine Acquirerbank des Händlers abgewickelt.

Rechnung per Kreditkarte oder Lastschrift[292] beglichen, bei T-Pay über die Telefonrechnung, deren Betrag in der Regel ebenfalls per Lastschrift eingezogen oder per Überweisung durch den Kunden bezahlt wird.

Das Prinzip der Billingverfahren wird am Beispiel Firstgate click & buy deutlich. Firstgate fungiert in Analogie zur Kreditkarte sowohl als Acquirer als auch als Issuer.[293] Das System ist seit 2000 am Markt, mittlerweile hat es nach eigenen Angaben 2500 Händler in verschiedenen Ländern und ca. 1,7 Millionen Kunden.[294] Die Händler werden von Firstgate betreut und auch hinsichtlich der angebotenen Inhalte überprüft. Umsätze, die der Händler über Firstgate erzielt, werden abzüglichlich der Umsatzprovision weitergereicht. Auf Händlerseite steht per SSL-Verbindung und Passwort ein geschützter Bereich bei Firstgate zur Verfügung, in dem Umsatz- und Transaktionszahlen eingesehen werdne können. Die Surfer, die per Firstgate bezahlen wollen, müssen sich einmalig registrieren (Name, Adresse, eMail, und Bankverbindung/Kreditkarte). Nach einer Plausibilitäts-/Missbrauchsprüfung und Bonitätscheck können Kunden bis zum vorgegebenen Limit im Internet einkaufen. Wird der Plausibilitätscheck (unter anderem syntaktische Überprüfung der Daten und Abgleich mit zugekauften Datensätzen) bestanden, erhalten Neukunden ein geringes Limit, bis zu dem sie sofort einkaufen können. Die Bonitätsüberprüfung findet parallel statt, zur Validierung der Bankverbindung wird den Kunden eine PIN per Überweisung von 10 Eurocent mitgeteilt. Dabei wird die Möglichkeit ausgenutzt, in der Betreffzeile einer Überweisung dem Kunden eine PIN anzugeben. Unter der Annahme, der Zugang zu den eigenen Kontoauszügen erfolgt exklusiv für den Bankkunden, ist ein Anscheinsbeweis für die Identität des Kontoinhabers erbracht. Erst wenn diese PIN auf der Firstgate-Internetseite eingegeben wurde, ist das Konto bis zum Bonitätslimit freigeschaltet. Bei Kreditkartenbezahlung wird eine Online-Autorisierung der Kreditkarte durchgeführt.

Eingekauft wird, indem auf Händlerseite der „Bezahlen mit Firstgate click & buy"-Button gewählt wird, und Passwort/Username, die bei der Anmeldung festgelegt werden, eingegeben werden. Optional kann die Passwort/Username-Kombination auch durch personalisierte X.509-Zertifikate oder IP-Fingerprints gewährleistet werden. Die Autorisierungsserver und der gesamte Datenverkehr der Firstgate Internet AG laufen über ein Hochsicherheitsrechenzentrum, unbefugte Zugriffe von außen sollen ausgeschlossen sein.[295] Erst nachdem die gewünschte Ware noch einmal von Firstgate mit dem dazugehörigen Preis auf einer Extraseite angezeigt und vom Kunden bestätigt wurde, gilt die Ware als bezahlt. Mit den Zugangsdaten wird auch auf Kundenseite der SSL-geschützte Servicebereich erreichbar, in dem unter anderem Transaktionsdaten eingesehen werden können. Passwort und Username sind auch auf Firstgate-Seite nicht einsehbar, lediglich der Kunde kennt diese Daten. Gehen sie verloren, kann über die Hotline ein neuer Zugang geschaltet werden. Für Missbrauch der Zugangsdaten haftet der Surfer. Die Bezahlung beim Händler erfolgt anonym, da mit dem Anklicken des Bezahlbuttons die Verbindung auf den Server von Firstgate umgelenkt wird, mit der Folge, dass der Händler nur weiss, dass Content abgerufen wurde, aber nicht von wem. Lediglich falls der Kunde die Rechnung nicht bezahlt, ermächtigt er Firstgate in den AGBs, die Adressdaten an den Leistungserbringer (Händler) weiter zu reichen. Das Routen der Verbindung über den Firstgate-Tarifierungsserver ermöglicht es dem System, ohne jede

[292] In der Regel einmal monatlich, bei höheren Umsätzen behält sich Firstgate vor, Abschlagszahlungen auch zwischendurch einzuziehen.
[293] Die Kooperation mit den Volks- und Raiffeisenbanken seit Mitte September, bei der sich deren Online-Banking-Kunden per PIN bei Firstgate anmelden können, erweitert das Modell. Die Volks- und Raiffeisenbanken wären in diesem Fall die Issuer – mit der Folge, dass für die Kundenvermittlung oder anteilig am Umsatz eine Erlösbeteiligung ausgehandelt werden kann (in Analogie zum Interbankenentgelt).
[294] Vgl. www.firstgate.de/wasist/wasist.html (09.09.2003).
[295] Vgl. Firstgate (2003).

Software auf Kundenseite auszukommen. Reklamationen werden von der Firstgate-Hotline bearbeitet, die auf die Transaktionsdaten zugreifen kann. Auf Händlerseite wird lediglich bei den kostenpflichtigen Angeboten ein Link zu den Firstgateseiten im Internetauftritt platziert. Die Tarifmodalitäten (Kosten pro Click, pro Zeiteinheit, Abonemment etc.) kann der Händler im Servicebereich selbst festlegen.

4.2.6.4.3 Rechnung mit Überweisung

Die Rechnung wurde bereits in 4.2.6.3.4 dargestellt. Wird nicht per Online-Überweisung in fast Echtzeit bezahlt, bleiben die Varianten der Online-Überweisung per Online-Banking-Modul oder die papiergebundene Überweisung. In beiden Fällen hat der Händler erst bei erfolgter Gutschrift die Gewissheit, dass er sein Geld erhalten hat. Somit werden diese Verfahren bei einigen Händlern und auch im Online-Auktionsgeschäft in der zeitlichen Abfolge umgekehrt. Der Käufer muss, will er die Ware erhalten, in Vorleistung treten und die Überweisung zunächst tätigen. Erhält er das Geld, wird die Ware inklusive Rechnung versendet. Damit wird der Kunde in die schwächere Position gesetzt und muss im Schadensfall per Zivilklage gegen den Verkäufer vorgehen. Ist der Kunde zu diesem Zeitpunkt insolvent, hat der Händler das Nachsehen.

Um das Problem der Informationsasymmetrie zu umgehen, haben sich treuhänderische Dienstleister etabliert. Beispielsweise hat die Sparkassengruppe einen Treuhanddienst (Sparkassen Internet Treuhand Service (S-ITT)) etabliert, der gegen Gebühr als unabhängiger Dritter den Eingang des Geldes und der Ware überwacht und erst im positiven Fall freigibt. Die Entwicklung des Systems am Markt verläuft von niedrigem Transaktionsniveau ausgehend positiv. Im März 2003 waren 15 Händler angeschlossen. Pro Monat wächst das System um ca. 10 Händler und 150 Neukunden.[296]

Eine Variante des Treuhandverfahrens findet sich mit dem Anbieter EuroCoin iclear GmbH (iclear). Die Gesellschaft ist hervorgegangen aus der iclear AG, die 2003 von der EuroCoin AG aufgekauft wurde. Nach Angaben von iclear nutzen Stand Sommer 2003 rund 1.000 Shops die Dienste des Unternehmens.Vor einer iclear-Zahltransaktion müssen Händler und Kunde bei iclear registriert sein. Konsumenten melden sich mit Bankverbindung/Kontonummer und eMail-Adresse an, Mindestalter sind 16 Jahre. Per eMail erhalten Neukunden Passwort und Benutzername, die den Zugang zu den iclear-Diensten ermöglichen. Die ersten Bestellungen akzeptiert iclear lediglich auf Vorauskasse und tritt somit als Treuhänder auf. Erst bei nachgewiesener Bonität, die über erfolgreiche Transaktionen aufgebaut wird, können Kunden auf Rechnung bezahlen.

Der Bestellvorgang von Waren und Dienstleistungen läuft für die Konsumenten über den Shop eines iclear-Vertragspartners. Für diesen Vertragspartner prüft iclear die Bonität des Kunden und gibt eine positive Bestätigung oder einen Warnhinweis an den Händler. Bestätigte physische Waren kann der Händler daraufhin sofort versenden und erhält eine Zahlungsgarantie durch iclear. Diese wird vertraglich so realisiert, dass bei einer Bestellung iclear als Zwischenhändler auftritt, dem Händler die Ware abkauft, und somit das Eigentum an den Waren bis zur Bezahlung an iclear übergeht (iclear als mittelbarer Besitzer[297]). Iclear betreibt damit kein Factoring, bei dem gegen Gebühr vom Factor die Forderungen des Factoring-Kunden an den Abnehmer der Waren (Kunden/Debitor) abgekauft werden. In der Sache kommt das iclear-Konzept dem offenen Factoring, bei dem der Kunde über das

[296] Vgl. Bauer (2003), S. 76.
[297] Vgl. Iclear (2003).

Abtreten der Forderung informiert wird, sehr nahe. Iclear erstellt die Rechnung im Auftrag des Vertragspartners sowohl für physische Waren (hier gilt die Zahlungsgarantie) als auch für digitale Inhalte (ohne Garantie). Iclear zieht die fälligen Beträge bei den Kunden per Lastschrift ein und überweist den Lieferanten diese nach Abzug der Gebühren. In den AGBs behält sich iclear vor, nicht für den Missbrauch der Zugangsdaten des Vertragspartners (Kunde) zu seinem über SSL-Verbindung gesicherten iclear-Konto oder andere Probleme mit und im Internet zu haften. Eine Sicherheit bietet im Schadensfall jedoch die Tatsache, dass physische Waren ausschließlich an die ursprünglich registrierte Adresse versendet werden können. Auf Händlerseite gilt für die Auslieferung physischer Waren eine vollständige Risikoübernahme der Bezahlung, sofern die Bestellung von iclear freigegeben wurde. Iclear verpflichtet sich, fällige Beträge spätestens 30 Tage nach Rechnungsstellung zu begleichen.

4.2.6.5 Risiken bei Retail-Bezahlverfahren

Aus Sicherheitsgründen ist die Frage von Relevanz, inwiefern es sich bei einem elektronischen Zahlungssystem um ein Zugangsprodukt oder ein „selbständiges" Verfahren handelt. Kann ein Verfahren korrumpiert werden, und wird dieser betrügerische Vorgang nicht vor dem Zugriff des Systems auf die Netze der Finanzinstitute entdeckt, besteht die Gefahr größerer Schäden. Diese Gefahr sinkt mit der Möglichkeit der transparenten Nachvollziehbarkeit jeden individuellen Prozessschrittes, der zum Initiator des Betrugs zurückführen kann. Gleichwohl kann bei anhaltender Betrugsmöglichkeit ein System von den Verbrauchern als unsicher empfunden werden, und bei neuen Systemen zu deren Misserfolg führen. Schlimmstenfalls überträgt sich das Gefühl der Unsicherheit auf andere im Kern sichere Verfahren in elektronischen offenen Netzen.

Eine solche Interpretation erscheint bei Analyse der Daten der Online-Umfrage „Internet-Zahlungssysteme aus Sicht der Verbraucher" (IZV6) zulässig. Obwohl lediglich unter 2 % der Konsumenten im Netz so schlechte Erfahrungen gemacht haben, fühlen sich über 50 % beim Einkaufen im Netz unsicher.[298] Dieses Gefühl der Unsicherheit könnte aus den negativen Berichten in den Medien unter anderem über Kreditkartenmissbrauch und Auktionsbetrügereien resultieren. Dabei zeigt IZV6 überraschenderweise für die Kreditkarte das Gegenteil: Die Kreditkartenbesitzer haben mit 0,6 % der Angaben noch seltener schlechte Erfahrungen gemacht und fühlen sich grundsätzlich sicherer bei Einkäufen im Netz als Personen, die von der Kreditkarte im Internet keinen Gebrauch machen wollen oder können.

Von den neueren Verfahren bedienen sich lediglich die Prepaid-Verfahren – solange sie durch Kauf einer physischen Karte mit Bargeld aktiviert werden – nicht der traditionellen Banken- und Kreditkarten-Zahlungsnetze. Bei der Nachnahme handelt es sich um eine Übergabe der Ware gegen Bargeld – solange (noch?) keine Zahlung mit der Debitkarte möglich ist. Gelingt es Betrügern, die Prepaid-Karten zu manipulieren, werden die emittierenden Firmen – nicht die treuhänderisch tätigen Finanzinstitute (solange kein Finanzinstitut eigene Karten emittiert) – geschädigt. Allerdings ist bei den beiden bekannten Prepaid-Karten, Paysafecard und Micromoney, bislang ein technischer Angriff auf die kryptographischen Grundlagen der Verfahren faktisch ausgeschlossen. Der Preis der Sicherheit ist ein relativ unkomfortables Eingeben 16-stelliger PINs. Zusätzlich lässt sich die Sicherheit bei der paysafecard weiter durch die Wahl eines optionalen Passworts erhöhen. Somit wird im physischen Verlustfall die Kartennummer wertlos – für den rechtmäßigen Besitzer, hat er sich die Nummer gemerkt/notiert – besteht bei Aufhebung der Anonymität die Möglichkeit, das verbleibende Guthaben zurückzuerhalten. Ein systemisches Risiko des Übergreifens von Schadensfällen auf Banken- oder Kreditkartennetze ist zu jedem Zeitpunkt ausgeschlossen; zumindest falls

[298] Leibold (2003), S. 39 ff.

die Karten nicht zukünftig virtuell werden (und damit der Distributionskanal potenziell angreifbar wird) und durch Online-Kanäle lediglich die PIN weitergeleitet wird.

Einen Sonderfall bildet die hardware-basierte GeldKarte. Deren Aufladevorgang kann zwar anonym erfolgen, die Transaktionen der GeldKarte jedoch werden auf einem Schattenkonto mitgebucht. Die bekannten Gefahren elektronischen Geldes, beispielsweise das Double-Spending bei Person-to-Person-Zahlungen, ist somit unkritisch. Erfolgreiche Angriffe auf die GeldKarte wurden bisher nicht dokumentiert. Die im ZKA formulierten Sicherheitsvorgaben sind teils zum Nachteil der schnellen Akzeptanz des Systems sehr hoch. Vermutlich sind Angriffe auch deshalb praktisch nicht dokumentiert, da der Aufwand zur Manipulation einer GeldKartenzahlung im Verhältnis zum potenziellen „Erfolg“ unverhältnismäßig hoch erscheint. Zudem sind mit der GeldKarte im Internet über Pilotanwendungen hinaus kaum Zahlungen mit der GeldKarte möglich.

Die Sicherheit der Kreditkartenzahlungen steigt mit den Verfahren zur eindeutigen Authentifizierung der Kreditkartenbesitzer. Reicht der physische Besitz der Karte oder einer Kopie in der physischen Welt aus, ist in der virtuellen Welt dann die reine Kreditkarteninformation (mit oder ohne CVC/CVV) wertlos. Die Problematik dürfte zumindest für die Übergangsfrist darin liegen, dass die Kreditkartenorganisationen Schwierigkeiten haben dürften, den Karteninhabern die Vorteile der neuen Verfahren nahe zu bringen. Solange der Verbraucherschutz eine starke Stellung einnimmt, und die Händler trotz Betrugsvorgängen weiterhin Waren per Kreditkarte verkaufen, ist der Anreiz für die Karteninhaber, sich an neue Verfahren zu gewöhnen (und für jeden Kreditkarteneinsatz eindeutig zu haften) eher als gering einzustufen.

Während im Individualzahlungsverkehr Kontenstände der beteiligten Akteure in Echtzeit endgültig verrechnet werden und die Beteiligten Ungereimtheiten schnell erkennen können, ist bei den Retail-Bezahlverfahren die Nähe des Bezahlzeitpunktes zur Warenübergabe ein entscheidender Sicherheitsfaktor. Allerdings mit der Einschränkung, dass ein Bezahlsystem oder der Zugang zu diesem nicht unbemerkt vom Besitzer kopiert werden kann. Im Fall der Kopie kann unter Umständen – insbesondere bei vorausbezahlten Systemen – die Sicherheit für die Händlerseite gegeben sein; betrogen wird der Verbraucher.

Von entscheidender Bedeutung für die Sicherheit der Bezahlsysteme im Retail-Bereich ist meist weniger die technische Ausgestaltung, sondern vielmehr die rechtliche Situation der Vertragspartner im Internet. Beispielsweise ist im Fall der Vorabüberweisung an einen Händler für den Verbraucher die Beweisbarkeit der Transaktion kein Problem. Ist der Händler unwillig oder unfähig (Konkurs) die gewünschte Ware zu liefern, bleibt dem Verbraucher der Gang zu Zivilgerichten, mit in der Regel mäßigen Aussichten auf Erfolg. Die Problematik der Legitimation des Zahlungskarteninhabers, wie sie bei Abhebungen an Geldautomaten ein häufiges Problem darstellt, wird bei Einsatz neuer Technologien geringer. Beispielsweise sind die neuen, auf kryptographischen Verfahren beruhenden, Zahlungssystemvarianten „Secure-Code“ und „Verified by Visa“ im Kreditkartensegment zumindest nach derzeitigem Wissensstand nicht zu korrumpieren – für die herkömmliche PIN bei Bargeldabhebung am Geldautomaten gilt diese Aussage weder für Kreditkarten noch für Debitkarten[299].

Ein Sicherheitproblem, mit dem die meisten Zugangsprodukte im Internet zu kämpfen haben, sind gefälschte Seiten, mittels derer versucht wird, diverse Zugangsinformationen vom Internet-Surfer zu erfragen. Dies kann mittels gefälschten eMail-Absenderadressen, gefälsch-

[299] Vgl. ausführlich mit Beispielen 5.3.2.1.1.

ten Internet-Links oder auch per Cross-Site-Scripting geschehen, und ist unter anderem bei Online-Banking-Zugängen und PayPal bereits mehrfach versucht worden. Die Gefahr des Missbrauchs ist dann besonders groß, wenn kein zusätzliches Geheimnis pro Transaktion (TAN) benötigt wird, sondern bereits nach dem Login Transaktionen ausgelöst werden können, beispielsweise bei PayPal.

Ein weiteres sicherheitskritisches Element stellt die allseits verwendete Verschlüsselungstechnologie dar, die bei der SSL-Kryptographie zum Einsatz kommt. Die SSL-Verschlüsselung ist im Internet zum de facto Standard geworden. Solange das Verfahren als sicher gilt und nicht kompromittiert werden kann, gibt es damit lediglich Verfahrensprobleme, die im folgenden beschrieben sind. Sollte jedoch die kryptographische Grundlage, der zugrundeliegende Verschlüsselungsalgorithmus mathematisch gelöst werden, würden auf einen Schlag sämtliche gängigen Verschlüsselungsprogramme obsolet. Da die Möglichkeit im laufenden Betrieb auf andere mathematische Probleme umzurüsten nicht besteht, würde die gesamte Internet-Kommunikation bedroht, nicht „nur" der Zahlungsverkehr.

Schmidt macht auf ein akuteres Problem im Umgang mit verschlüsselten SSL-Verbindungen aufmerksam.[300] Das Grundprinzip einer SSL-Verschlüsselung beruht auf der senderseitigen Verschlüsselung von Daten mit einem kryptographischen Schlüssel. Da es sich um ein assymmetrisches Verfahren handelt, muss dazu der öffentliche Schlüssel des Empfängers verwendet werden. In der Folge kann mit dem privaten Schlüssel des Empfängers dieser die Nachricht entschlüsseln. Das Problem liegt in der Übertragung des öffentlichen Schlüssels. Gelingt es einem Angreifer, seinen Schlüssel einzuschleusen, ist die gesamte Verschlüsselung hinfällig. Bei einer SSL-Kommunikation wird der zu übergebende Schlüssel in einem Zertifikat untergebracht, das den Klarnamen des Inhabers enthält, bestätigt mit der digitalen und damit nachprüfbarer Unterschrift des Zertifikatausstellers, beispielsweise Verisign. Beim Aufbau einer https-Verbindung (die SSL-Verschlüsselung benutzt) überprüft der Internet-Browser das zu dieser Seite gültige Zertifikat, das Verfallsdatum desselben und die digitale Unterschrift. Nur wenn alle Bedingungen erfüllt sind, wird die Verbindung aufgebaut. Ansonsten erfolgt eine Warnung. Da laut Schmidt die Programmierung vieler Internet-Seiten, auch https-Seiten, nicht gut ist, liefern SSL-Verbindungen auch bei korrekten Seiten überproportional viele Fehlermeldungen. In der Folge ignorien die Anwender die Warnungen, bauen die Verbindung trotzdem auf, und laufen Gefahr bei betrügerischen (Umleitungs-) Seiten zu landen.

Diese Gefahr ist insbesondere im Zahlungsverkehr nicht zu unterschätzen, da Angreifer mit einer falschen Verbindung leicht die daraufhin eingegebenen Zugangsdaten beispielsweise zu Systemen wie PayPal bekommen. Ist zusätzlich die Seite so aufgebaut, dass im Hintergrund die Daten an die korrekte Seite weitergeleitet werden, merkt der ahnungslose Anwender noch nicht einmal den Verlust vertraulicher Daten – für deren missbräuchlichen Einsatz er gemäß AGBs der meisten Firmen haftet.

Im Großzahlungsverkehr ist diese Gefahr aufgrund der höheren Sicherheitsvorkehrungen und zusätzlicher proprietärer Verschlüsselungen so nicht gegeben. Der B2B- und B2C-Handel jedoch sind zumindest potenziell gefährdet.

4.3 Akteure und ihre strategischen Rollen im Zahlungsverkehr

Zahlungsverkehr ist in immer stärkerem Maße ein technologiegetriebener Wirtschaftszweig. Dies gilt nicht nur für den eCommerce und mCommerce und damit internetbasierte Zahlungs-

[300] Vgl. Schmidt (2003).

verkehrsdienstleistungen, es gilt in fast gleicher Intensität auch für den stationären Handel (Point of Sale) und die Back-Office-Applikationen der Banken.[301]

Es kommt zu einer Veränderung herkömmlicher Wertschöpfungsketten.[302] Schlueter und Shaw beschreiben diese Veränderung für die sogenannten Digital Interactive Services[303], indem sie der konventionellen Wertschöpfungskette, auf der die Waren und Dienstleistungen geschaffen werden, noch eine parallele zweite Ebene, die Infrastrukturebene, hinzufügen. Auf der Infrastrukturebene finden sich die technologieorientierten Dienstleister, unter anderem Telekommunikationsunternehmen, die als Netzbetreiber fungieren, aber auch Zahlungssystem-Dienstleister, die bestimmte Plattformen beispielsweise zur Kontenaggregation betreiben. Geyer-Schulz et al. haben dieses Modell der Wertschöpfungskette auf den Markt für digitale wissenschaftliche Informationsgüter angewendet und konnten deutliche strukturelle Veränderungen auf diesem Markt nachweisen.[304] Andere Autoren sprechen im Zusammenhang mit dieser Entwicklung von konvergierenden Wertschöpfungsketten einzelner Industrien, beispielsweise IT-Industrie, Telekommunikation, Medien, Finanzdienstleistungen, die in Zukunft nicht mehr so einfach wie in der Vergangenheit separiert werden können.[305] Eine Entwicklung, die durch die Deregulierung technologiegetriebener Märkte wie der Telekommunikation weiter begünstigt wird.

In Abbildung 15 wird der Sachverhalt der konvergierenden Wertschöpfungsketten in der Darstellung eines Wertschöpfungsnetzes am Beispiel mobiler Dienstleistungen dargestellt und verdeutlicht die Komplexität der Beziehungen einzelner Industrien zueinander. Der European Communication Council schließt daraus[306]: „Eine funktionale Aufteilung von Produkt-Markt-Kombinationen ist aufgrund der zunehmenden Vernetzung bislang getrennter Segmente, die die Komplexität der Wettbewerbsverhältnisse erhöht, nur noch schwer aufrecht zu halten."

Im Rahmen der vorliegenden Arbeit gilt es darzustellen, welche Akteure auf dem Markt für Zahlungsverkehr tätig sind, welche Machtpositionen sie darin einnehmen, und welchen Stellenwert sicherheitsrelevante Fragestellungen für die einzelnen Akteure haben.

Ein geeignetes Konzept für diese Darstellung bietet eine Analyse nach strategischen Gruppierungen.[307] Strategische Gruppierungen sind nach Porter[308] „eine Gruppe von Unternehmen in einer Branche, die dieselbe oder ähnliche Strategie – entsprechend ihrer strategischen Dimensionen – verfolgen." Dabei werden die Akteure im sogenannten „Competitive Radar" auf ihre Wettbewerbs- und Angebotspositionen hin untersucht (siehe Abbildung 16).

[301] Vgl. Krueger (2001), S. 9 f.
[302] Vgl. Schlueter (1997).
[303] Definition in Schlüter (1997), S. 20: „Digital Interactive Services provides interactive, integrated information, and education, communication, transaction, and entertainment services on demand."
[304] Vgl. ausführlich Geyer-Schulz (2003).
[305] Vgl. Zederick (1999), S. 174.
[306] Zederick (1999), S. 129.
[307] Die folgenden Ausführungen basieren wesentlich auf Hennig (2002), S. 56ff.
[308] Porter (1992), S. 177.

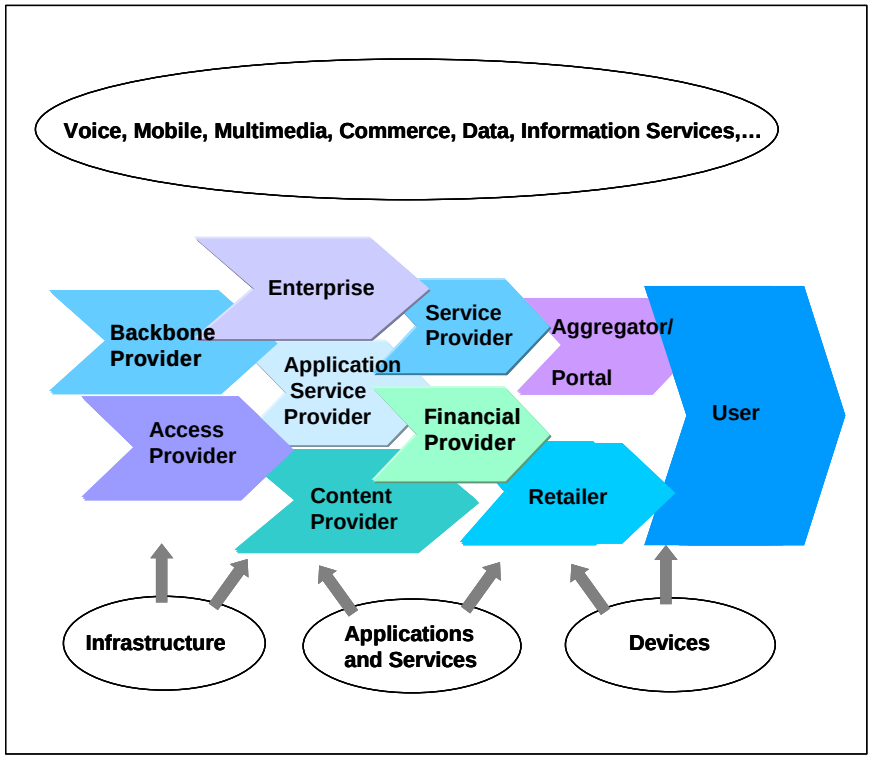

Abbildung 15: Wertschöpfungsnetz am Beispiel mobiler Dienstleistungen[309]

Die Unternehmensgruppierungen besetzen, ausgehend von einem Hauptmerkmal, verschiedene Felder in Bezug auf Infrastruktur, Finanzen (Zahlungsverkehr), Dienstleistungen im weiteren Sinne und Technologieentwicklung oder -bereitstellung. Die Infrastruktur nimmt im Zeitalter der Digitalisierung über die Bereitstellung leistungsfähiger Netzwerke eine wesentliche Rolle ein. Unter Finanzen werden die Dienstleistungen und Produkte mit direktem Bezug zum Bezahlen angenommen. Dienstleistungen stellen das Produktsegment dar, in dem für Endkunden und Zwischenkunden Leistungen erbracht werden, die Zahlungsdienstleistungen erst ermöglichen oder aber benötigen. Die Technologieachse kennzeichnet die Industrien, die hard- und softwarebasiert Produkte entwickeln, vertreiben und warten, mit denen in Kombination mit den elektronischen Netzen bestimmte Zahlungssystemprodukte und -dienste (und die Notwendigkeit, diese auch einzusetzen) erst möglich werden.

Die relevanten Unternehmensgruppierungen, die auf ihre strategische Positionierung hin in Grundzügen analysiert werden sollen, sind im Einzelnen:

- Finanzinstitute mit Banken, Sparkassen und Kreditkartenunternehmen,
- Payment Service Provider mit Anbietern neuer Verfahren und Billing/Clearing-Funktionalitäten,
- Netzwerkbetreiber mit den Telefongesellschaften und Service Providern und
- Dienstleistungsunternehmen insbesondere Distributoren aber auch Anbieter neuer Dienste wie Auktionshäuser.

Der Vollständigkeit halber sind Systemintegratoren wie beispielsweise die Beratungsunternehmen Accenture, Cap Gemini und CSC Ploenzke und Technologielieferanten, wie IBM, Nokia und Microsoft, aufgeführt. Letztere gestalten den Markt für Zahlungsverkehr durch die Art und den Umfang der angebotenen und eingeführten Technologien entscheidend

[309] Hennig (2002), S. 50.

mit. Beispielsweise ist die Entscheidung, aufgrund mangelnder attraktiver Kooperationen auf ein Dual-Slot-Handy in der Massenanwendung zu verzichten, sicherlich eine marktprägende Entscheidung gewesen. Hätten die Finanzinstitute über einen speziellen Chip die Authentisierungsmöglichkeiten für den Zugang zu ihren Zahlungsverkehrs-Netzwerken gehabt, wäre unter Umständen das mobile Bezahlen einen anderen Weg gegangen.

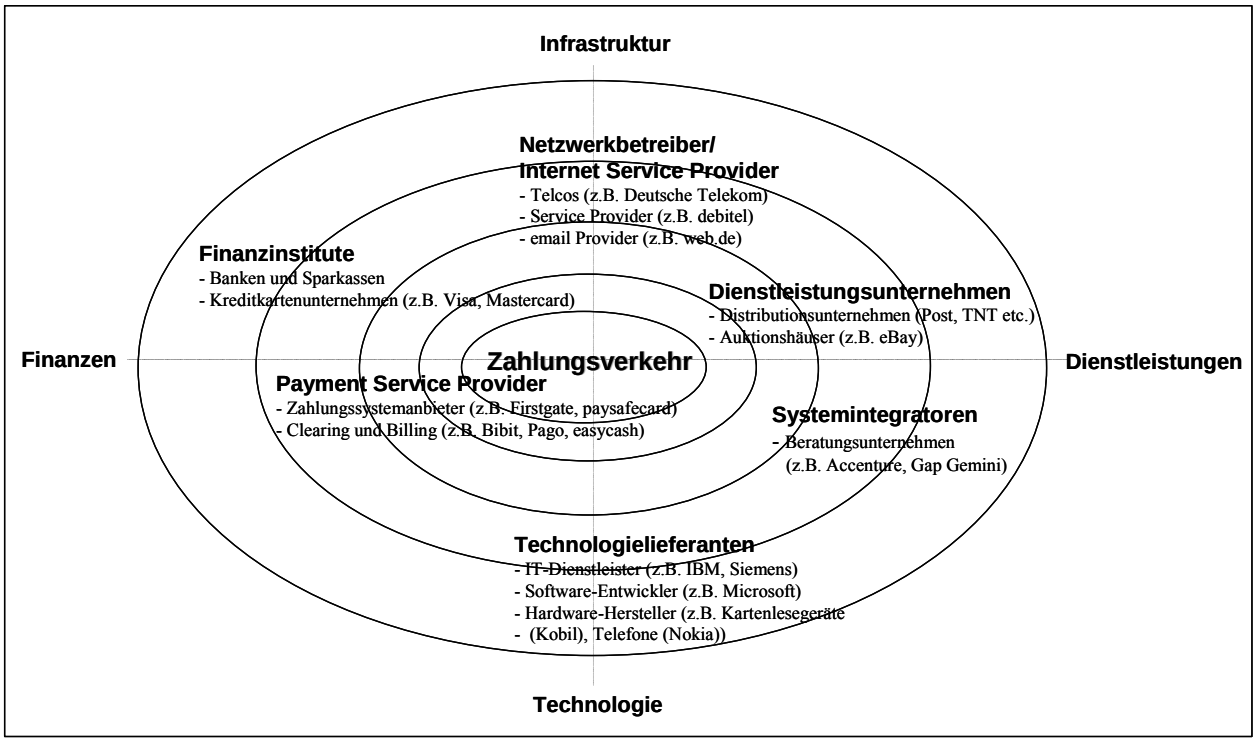

Abbildung 16: „Competitive Radar" der strategischen Unternehmensgruppierungen im Markt für Zahlungsverkehr

Die Beratungsunternehmen sind einerseits bei der konzeptionellen Planung einzelner Dienstleistungen und Produkte und andererseits als Ideenlieferant technologisch avancierter Produkte nicht zu unterschätzen. In jüngster Zeit kam es dabei zu interessanten Partnerschaften. Beispielsweise versuchte die Deutsche Bank mit Accenture im Rahmen eines Joint Ventures, die Firma Stackbox aufzubauen, die eine neue Technologie für elektronische Überweisungen und Kontenaggregation vertreiben sollte.[310]

Nicht in der Abbildung aufgeführt, da in diesem Sinne kein Unternehmen, aber von ebenso großer Bedeutung sind einerseits die Aufsichtsorgane und Regulierer, die das Angebot und Zusammenspiel der Unternehmensgruppen beaufsichtigen, regulieren und teils mitgestalten und andererseits die Konsumenten. Über ihre Nachfragemacht gestalten die Endverbraucher mit ihrem Akzeptanzverhalten indirekt auch die Nachfrage nach den relevanten Zwischenprodukten (Software, Terminals, Zahlungsverkehrsprodukte und -dienstleistungen) in diesen Märkten. Eine Erkenntnis, die unter anderem für die Hersteller von Kartenlesegeräten für die GeldKarte aufgrund fehlender Nachfrage unangenehme Konsequenzen hatte.

Porter erkennt bereits lange vor Erreichen des Höhepunkts der Internet-Euphorie die Schwierigkeit an, in Wirtschaftssektoren und -bereichen die Märkte und Akteure mit ihren Aufgaben und Grenzen zu identifizieren. Diese Aufgabe ist mit der Vernetzung digitalisierter

[310] Mittlerweile ist die Produktpalette der Stackbox im Zuge von Konsolidierungsbemühungen bei einer anderen Tochter der Deutschen Bank, Pago eTransaction Services GmbH, integriert.

Prozesse nicht einfacher geworden. Gleichwohl kann, wie in der strukturellen Darstellung in Abbildung 16 geschehen, anhand der wesentlichen Kenngrößen eine strategische Gruppierung vorgenommen werden. Diese ermöglicht im Anschluss eine Interpretation der Märkte im Sinne einer ersten Abschätzung, in welche Richtung sich die Akteure im elektronischen Zahlungsverkehr strategisch ausrichten könnten.

Die strategischen Dimensionen, an denen Porter die Wettbewerbsstrategie von Akteuren misst, umfassen ein ganzes Bündel und sind für die Zwecke dieser Arbeit nur bedingt von Interesse. Porter berücksichtigt unter anderem den Grad der Spezialisierung, die Markenidentifikation, die Wahl des Vertriebswegs, die Produktqualität, das Ausmaß an entwickelten Zusatzdienstleistungen, die Preispolitik und die Beziehung zum Gesamtunternehmen aber auch zu lokalen und ausländischen Regierungen.[311]

Einen Einblick in die Problematik des Marktes für Zahlungssysteme und -dienstleistungen und die Positionierung der Akteure erhält man bereits mit einem konzentrierten Bündel an strategischen Dimensionen. Im einzelnen wird bei der Analyse der Akteure auf folgende Dimensionen einzugehen sein:

- *Spezialisierung*: Inwieweit ist ein Unternehmen auf seine Kernkompetenzen konzentriert und welche Rolle spielen Innovationen?
- *Technologievorsprung*: Wie stehen die Akteure zu Innovationen, generell aber auch zu Fragen der Technologieführerschaft, die allerdings dann auch den Kunden so vermittelt werden muss?
- *Netzwerk*: In welcher Form gehen die Unternehmen Allianzen ein, integrieren Produkte und Dienstleistungen entlang ihrer eigenen Produktion/Dienstleistungen?
- *„Macht":* Kann ein Unternehmen den Markt maßgeblich gestalten? Inwiefern kann es Einfluss auf die anderen Akteure nehmen?

Im Kontext der vorliegenden Untersuchung sind zwei weitere Dimensionen von Bedeutung:

- *Sicherheit*: Welchen Bezug zu sicherheitsrelevanten Fragestellungen hat das Unternehmen?
- *Beziehungen zur Aufsicht*: Wie ist das Unternehmen hinsichtlich (bank-)aufsichtlichen Themen aufgestellt?

4.3.1 Finanzinstitute

Bei den Finanzinstituten sind neben den Geschäftsbanken und Sparkassen im Bereich Zahlungsverkehr die Kreditkartengesellschaften, in Europa namentlich Visa und Mastercard von großer Bedeutung. Diese Organisationen betreiben im Wesentlichen den bargeldlosen Zahlungsverkehr. Durch die Elektronisierung ist ihr Geschäftsfeld, was die Möglichkeit neuer Produkte und Dienstleistungen aber auch „economies of scale" angeht, stark in Bewegung und es versuchen neue Dienstleister, in angestammte Bereiche vorzudringen.[312]

4.3.1.1 Geschäftsbanken und Sparkassen

Im klassischen Geschäft der Banken und Sparkassen, der Risiko- und Fristentransformation, fungieren diese als Intermediäre. Durch die Technisierung nicht allein der Finanzwelt,

[311] Vgl. Porter (1992), S. 174 ff.
[312] Vgl. ausführlich aus Sicht der Banken und Sparkassen Rehm (2001), S. 13 ff. Aus Sicht der Deutschen Bundesbank Friederich (2001).

sondern auch der Außenbezüge bis hin zu den Kunden mit PCs, ergibt sich für Dienstleister die Chance, zwischen Bank und Kunden in die Wertschöpfungskette „einzudringen". Beispielsweise können Zahlungssystemanbieter und –dienstleister wie die Firstgate Internet AG die Beträge aggregieren oder auch kartenausgebende Instanzen, wie das Handelsunternehmen KarstadtQuelle AG, Prozessoren bis hin zu Software-Firmen und anderen Akteuren. Die Folge: Es kommt zur Disintermediation.[313] Diese wird vor allem an den Stellen für die Wertschöpfungstätigkeit der Banken zur Gefahr, an denen die neuen Anbieter zu nah an das traditionelle Bankgeschäft oder die Infrastruktur der Finanzinstitute herankommen.

Ein gutes Beispiel lieferten die im Frühsommer 2003 stattfindenden Streitigkeiten, ob T-Online, die Online-Überweisung über seine Plattform in dieser Form, nämlich ohne Kooperationsabkommen mit Finanzinstituten, überhaupt abwickeln darf. T-Online bietet in ausgewählten Shops (u.a. ARD-Fernsehlotterie, T-Online Shop, T-Online Ticket Shop) die Möglichkeit mit HomePay, einer Online-Überweisungs-Lösung der Firma fun communications, einzukaufen. Die Pläne der im ZKA vereinten Bankengruppen, dieses Bezahlverfahren abzumahnen (die Postbank bietet Händlern das baugleiche Verfahren an), zeigen, dass offensichtlich eine Telekommunikationsfirma zu nahe an das Stammgeschäft, Online-Banking, der gesamten Kreditwirtschaft herangeraten ist. Bis Frühjahr 2004 ist jedoch zu keiner offiziellen Abmahnung gekommen. Die Branche scheint sich auf den neuen Status quo einzustellen.

Spezialisierung
Auf der anderen Seite versuchen auch die Finanzinstitute, zunehmend neue Wertschöpfungsketten zu erschließen. Wesentliche Impulse gehen dabei von der angestammten Position der Banken als glaubwürdiger Mittlerinstanz aus. Banken bieten „trusted services" an, z. B. das Treuhandverfahren der Sparkasse für den Handel und Auktionen im Internet[314] oder versuchen, Public Key-Infrastrukturen aufzubauen und zu betreiben, beispielsweise mithilfe der im Besitz internationaler Banken befindlichen Identrus LLC[315]. Im Zahlungsverkehr findet zunehmend der Versuch statt, die Rolle des Payment Service Providers, der eigene Zahlungssystem-Plattformen betreibt und zusätzliche Dienstleistungen anbietet, einzunehmen. Beispielsweise bietet die Postbank mit „Postbank-Pay-Solutions" eine modulare Plattform für Zahlungssystem-Dienstleistungen an, die auch aktiv an Händler vertrieben wird. Analoge Bemühungen lassen sich im Sparkassensektor und bei den Genossenschaftsbanken beobachten, dort kommt es teilweise bereits zu Kooperationen.

Technologieführerschaft
Die technologische Entwicklung bewirkt auch bei den Finanzinstituten zunehmend den Einsatz neuer Technologien. Deren Einsatz wird aber nicht im Sinne eines Marketingeinsatzes in Richtung Kunden betont, vielmehr verändert sich die Back-Office-Landschaft zunehmend. In jüngster Zeit konnte allerdings mit dem Aufkommen der Direktbanken im Aktienboom neue Technik auch kundennah angebracht und im Sinne von Technologieführerschaft beworben werden. Für die Institute ist jedoch der mit diesen Technologien schnelle Zugang der Kunden zu den Finanzdienstleistungen mit dem Risiko des ebenso schnellen Wechsels der Bankverbindung bei besseren Konditionen verbunden. Je nach Vertragsgestaltung und Attraktivität der „herkömmlichen" Banken wird diese Tendenz bestärkt oder konterkariert.

[313] Vgl. O'Brien (2000), S. 51 und Hennig (2002), S. 61 f.
[314] Vgl. Geisinger (2001).
[315] Vgl. www.identrus.com und weiterführend zu Public Key Infrastrukturen bei Finanzinstituten Hruby (2002).

Netzwerk
Der Aufbau von Netzwerken nimmt in der Finanzwelt zu, im Zahlungsverkehr ist die Cash Group, die den kostenlosen Gebrauch von Geldautomaten der teilnehmenden Institute für die Kunden ermöglicht, ein Beispiel. Bei den durch mögliche „economies of scale" induzierten Veränderungen im Back-Office gibt es jedoch Schwierigkeiten. Der Aufbau von Transaktionsbanken, die europaweit agieren könnten, verzögert sich. Problemfelder sind einerseits die fehlende Zuordnung des Kunden zur jeweiligen Hausbank (Wertschöpfungsanteil zuordnen) andererseits die notwendige Einigung auf eine gemeinsame Plattform/Technologie.

Institutsintern kommt es zur Zeit zu einem engeren Zusammengehen von Technologielieferanten, Dienstleistern und Finanzinstituten. Der Outsourcing-Auftrag weiter Teile der IT-Umgebung der Deutschen Bank an IBM deutet an, dass die jeweiligen Akteure ihre Kernkompetenzen ausbauen, und dafür im operativen Geschäft in engeren Netzwerken verknüpft sind.

Größere Unwägbarkeiten gibt es im Bereich von Kooperationen der Finanzinstitute mit anderen Akteuren. Die angestrebten Verbindungen von Banken und Telekommunikationsunternehmen, die interessante Möglichkeiten eröffnet hätten, sind vorerst gescheitert. Prominente Beispiele waren das im Februar 2002 eingestellte Joint Venture MobilBank zwischen der Landesbank Baden-Württemberg und der MobilCom AG und das im August 2002 eingestellte Joint Venture memIQ der HypoVereinsbank AG und der Vodafone Group plc, bei dem eine auf der digitalen Signatur beruhende Archivierung von Kontoauszügen realisiert wurde.

Sicherheit
Zahlungsverkehr und Sicherheit sind Kernkompetenzen der Branche. Vertrauen in die Finanzbranche ist überlebenswichtig. Gleichwohl zeigen die Diskussionen um Operationelle Risiken in Basel II, dass es im Bereich Risikomanagement noch Verbesserungsmöglichkeiten gibt. Die geringe Anzahl an gravierenden Schadensfällen, die nach außen dringen, zeigt jedoch, dass es bisher der Branche gelungen ist, trotz Einsatz von Computertechnologien im großen Stil, deren Sicherheitslücken nicht zu ihrem eigenen Problem werden zu lassen. Ein Grund für diesen Erfolg kann im vorsichtigen Einsatz neuer Technologien, insbesondere wenn sie bei Kunden eingesetzt werden, gesehen werden. Auf der institutionellen Seite ist der ZKA neben den bankinternen Bemühungen und dem Hinzuziehen von externen Experten in dieser Hinsicht eine wirkungsvolle Instanz bei der Freigabe bestimmter sicherheitskritischer Technologien, sei es im Home-Banking-Bereich (obwohl in Einzelfällen auch dort von Problemen berichtet wird), bei der Technologie für Geldausgabeautomaten oder bei technologischen Komponenten der GeldKarte.

Macht
Bei aller Marktdiversifizierung und der zumeist technologiebedingten Existenz neuer Akteure auf dem Markt für Zahlungsverkehr bleibt eines festzuhalten: das Settlement von Zahlungen bleibt in allen Fällen den Finanzinstituten vorbehalten, als klassisches bankerlaubnispflichtiges Geschäft nach § 1 Abs. 1 KWG. Damit bleiben die Kreditinstitute in diesem Geschäft unangreifbar, einzig der Wettbewerb aus dem europäischen Ausland könnte für Bewegung sorgen. Erste Ansätze zeigen sich an dieser Stelle. Eine englische Kapitalgesellschaft hat als erste erfolgreich eine eingeschränkte Banklizenz als E-Geld-Institut auf Grundlage der EU-Richtlinie 2000/46/EG[316] erhalten und wirbt damit europaweit. Mit dem Erwerb der e-Banklizenz wird Moneybookers zum Finanzinstitut mit eingeschränkten Möglichkeiten. Aus strategischer Sicht ist von Bedeutung, dass die Eigentümer von Moneybookers keine

[316] Vgl. EU (2000). Genauere Ausführungen zur Bedeutung der Richtlinie u.a. bei Heitmann (2002), S. 278ff.

Finanzinstitute sind, wie dies beispielsweise bei der Kreditkartenbranche der Fall ist und durch eine Beteiligung der Deutschen Bank auch bei Paybox der Fall war. Die Geschäftstidee von Moneybookers ähnelt dem PayPal-Verfahren. Es wird für die Verbraucher mittels eMail möglich, kostengünstig und einfach Geld zu versenden.[317]

Die Macht, neue Geschäftsfelder außerhalb der angestammten Bereiche zu besetzen, ist begrenzt. Die Schwierigkeiten der Finanzinstitute, die Akzeptanz der GeldKarte voranzutreiben, zeigen die begrenzten Möglichkeiten, insbesondere bei möglicherweise divergierenden Interessen einzelner Verbände innerhalb der Branche.

Die Problematik der GeldKarte macht auch deutlich, dass der Netzwerkcharakter der Finanzindustrie in Bezug auf tragfähige Verbindungen in andere Industrien relativ wenig ausgeprägt ist. Nur so lässt sich die geringe Anzahl an Applikationen für die GeldKarte erklären.

Beziehungen zur Aufsicht
Die Kreditwirtschaft ist eine im Wettbewerbsrecht privilegierte Branche, nicht zuletzt aufgrund der systemischen Risiken, denen die Finanzwelt ausgesetzt ist. Die Branche unterliegt der stärksten aufsichtlichen Beobachtung und Kontrolle aller aufgeführten Akteure. Mit Basel II wird erstmalig der Versuch unternommen, auch im Bereich der Operationellen Risiken finanzielle Anreize für die Marktteilnehmer zu schaffen, fortgeschrittene Risikomanagement-Systeme zu implementieren. Damit wird ein Stück von der reinen Lehre der Verordnungen und Kontrolle abgerückt. Hinzu kommt der Versuch, mit, wenn auch bescheidenen, Offenlegungspflichten für mehr wettbewerblichen Druck auf die Marktteilnehmer zu sorgen.

In Deutschland sind die Verbindungen der Kreditinstitute zur Aufsicht gerade unter dem Aspekt der Sicherheit als relativ gut zu klassifizieren. Mit der brancheneigenen Institution ZKA hat die Aufsicht einen geeigneten Ansprechpartner für die Diskussion relevanter Themen. Die Zahlungsverkehrsabkommen, bei denen die Kreditinstitute mit der Deutschen Bundesbank als Betreiberin eigener Zahlungssysteme Absprachen treffen, werden im ZKA koordiniert.

4.3.1.2 Kreditkartenunternehmen

In Deutschland sind die bekanntesten Kreditkartenunternehmen mit den meisten ausgegebenen Kreditkarten MasterCard mit knapp über 50 % Marktanteil und VISA mit ca. 40 % Marktanteil, Diners Club liegt als drittes Unternehmen bei ca. 8 %.[318]

Visa International ist eine Organisation mit weltweit über 21.000 Mitgliedsbanken. Mehr als eine Milliarde Visa-Zahlkarten sind weltweit im Umlauf und können in über 150 Ländern an über 30 Mio. Akzeptanzstellen, darunter 810.000 Geldautomaten, eingesetzt werden.[319] 2002 betrug der Umsatz der mit Visa-Karten gekauften Güter und Dienstleistungen 2.400 Mrd. US-$.[320] Visa International ist in sechs regionale Organisationen aufgegliedert, eine davon ist VISA EU in der Europäischen Union.

[317] Vgl. Moneybookers (2003) und 4.2.6.3.5.
[318] Vgl. www.visa.de.
[319] o.V. (2003g).
[320] http://corporate.visa.com/av/main.shtml (10.09.2003).

MasterCard International hatte bis 2002 die gleiche Organisationsstruktur wie Visa. Im Juni 2002 wurde eine Aktiengesellschaft (nicht börsengehandelt) MasterCard Incorporated gegründet, deren Anteilseigner weltweit ungefähr 25.000 Finanzorganisationen sind. Die wichtigste Gesellschaft der Holdinggesellschaft MasterCard Incorporate ist die MasterCard International, die das Kredit- und Debitkartengeschäft (mehr als 1 Mrd. Karten im Umlauf) betreibt. Mit 32 Mio. Akzeptanzstellen und 892.000 Geldautomaten in 210 Ländern bezeichnet sich MasterCard als größte Kartenorganisation.[321] Der Umsatz lag 2002 bei rund 2.000 Mrd. US-$.

Die Kreditkartenzahlung hat in Deutschland und Europa nicht den Stellenwert, den sie in den USA erreicht hat, ist aber gleichwohl im eCommerce, besonders im grenzüberschreitenden, das weitverbreitetste Zahlungsmittel mit starken Wachstumsraten. Beispielsweise konnte Visa im letzten Quartal 2002 die Umsätze im Internet gegenüber dem Vorjahreszeitraum verdoppeln.[322]

Spezialisierung
Die Kreditkartengesellschaften haben sich auf die Zahlung mit Karten jeder Art, vornehmlich Kreditkarten aber auch Debitkarten, spezialisiert. Eine Diversifikation kann hier nur schwierig greifen, am ehesten noch mit Zusatzdienstleistungen, die an den Besitz und Einsatz der Karte anknüpfen, beispielsweise Versicherungen jeder Art oder Bonuspunkte/-meilen.

Eine kritische Größe ist die Altersbeschränkung, die den Einsatz von Kreditkarten für Jugendliche schwierig gestaltet. Visa versucht, mit Visa Buxx[323] eine Karte am Markt zu platzieren, die als eine Art Prepaid-Kreditkarte aufgestellt ist und speziell diesen potenziellen Kundenkreis ansprechen soll. Visa versucht, dabei den pädagogischen Umgang mit Geld in den Vordergrund zu stellen und macht gleichzeitig mit der Sicherheit einer Kreditkarte gegenüber Bargeld Werbung. Ein Konzept, das bei der Verbreitung der Kreditkarte in den USA aufgehen kann, in Europa und besonders in Deutschland wohl kaum Chancen haben dürfte.

Kreditkarten in Deutschland sind im eigentlichen Wortsinn keine Kreditkarten, da zwar Ausgaben während eines Abrechnungszeitraums, in der Regel ein Monat, summiert werden, aber nach Ablauf dieses Zeitraums der Betrag von einem Girokonto beglichen wird. Der Begriff Inkasso-Card wäre für dieses Produkt angemessener. Erst die in jüngster Zeit beworbenen Revolving Credit Cards haben die eigentliche Kreditkartenfunktionalität. Nur ein Teil der Summe wird am Ende des Abrechnungszeitraums vom Kunden bezahlt, der Rest bleibt als zinspflichtiger Kredit mit monatlichen Zins- und Rückzahlungen stehen.

Technologieführerschaft
Der Betrieb eines weltweiten Clearing- und Settlementnetzes für Kreditkartenzahlungen bedingt, um konkurrenzfähig zu bleiben, den Einsatz ausgereifter Technologien. Die notwendige Installation von Technologie am Point of Sale verdeutlicht aber auch die Schwierigkeit kurze Innovations- und Lebenszyklen zu realisieren. Diese Schwierigkeit wird anschaulich, beim Versuch der Kreditkartengesellschaften, die Basistechnologie der Kreditkarten von Magnetstreifen auf Chipkarten umzustellen. Diesem Entschluss gingen weltweite zähe Verhandlungen und notwendige Vertragsanpassungen voraus, die die Einführung der neuen Technologie im Vergleich zur technischen Machbarkeit vermutlich um Jahre nach hinten verlegt haben. Ein wesentliches Problem ist dabei der Netzwerkcharakter.

[321] www.mastercardintl.com/newsroom/faqs.html (10.09.2003).
[322] Vgl. o.V. (2003g).
[323] Vgl. www.visabuxx.com.

Da die Kreditkartenunternehmen im Netzwerk agieren, haben sie beispielsweise keinen Zugriff auf Investitionsentscheidungen der Händler. Somit können sie die Finanzierbarkeit eines neuen Terminals, das beispielsweise in der Lage ist, Chipkarten auszulesen, nur indirekt vorantreiben. Der Einsatz kostenintensiver neuer Technologien, beispielsweise die Umrüstung auf Terminals, die EMV-Chips lesen können, muss in der Folge von den Kreditkartenorganisationen im Einvernehmen beschlossen und teilsubventioniert werden. Visa unterstützt die Einführung der EMV-Technologie auf Seiten der Händler, Banken und Lieferanten mit 168 Mio. Euro.[324]

Auf Kundenseite versuchen die Kreditkartengesellschaften gleichwohl den Eindruck äußerster Flexibilität und Zukunftsorientiertheit zu vermitteln. Die Botschaft, die in der Werbung vermittelt wird, lautet, es ist „in" und zukunftsorientiert, mit einer Kreditkarte zu bezahlen.

Netzwerk

Der Erfolg von Kreditkartenunternehmen beruht auf dem Aufbau eines funktionierenden weltweiten Netzwerks. In dieser Hinsicht sind Kreditkartenorganisationen neben den Telefongesellschaften die Musterbeispiele für ein Überwinden der Henne-Ei-Problematik. Durch die systembedingte Trennung in Issuer und Acquirer wird das Netzwerk noch zusätzlich ausgedehnt. Vom Endkunden über die Banken hin zum Händler verfügen Kreditkartenunternehmen über das wohl größte Netzwerk im eigentlichen Wortsinn der Welt.

VisaNet, das Abrechnungsnetz von Visa International, bezeichnet sich als größten gewerblichen Abrechnungsservice für den Zahlungsverkehr.[325] BankNet des Konkurrenten MasterCard International steht dem in nichts nach, und sieht sich als „one of the world's largest global telecommunications networks"[326], in dem die Mitglieder von MasterCard mit den Datenverarbeitungszentren verbunden werden.[327] Der technologische Aufbau der Netzwerke beider Anbieter ist ähnlich. MasterCard bediente sich als erster großer Netzbetreiber bereits 1997 in Zusammenarbeit mit dem Telekommunikationsunternehmen AT&T der Technologie eines TCP/IP[328]-basierten Virtual Private Network (VPN), in dem die Kommunikation über offene Netze verschlüsselt und sicher gegen äußere Angriffe erfolgen kann. Der Authorisierungsprozess bei einer Kartenzahlung wird von MasterCard im Durchschnitt in 130 Millisekunden abgewickelt – gegenüber 650 Millisekunden vor der Einführung der VPN-Struktur. An den transaktionsreichsten Tagen des Jahres 2002 wurden im System pro Tag 36 Mio. Kreditkarten- und 40 Mio. Debitkartenanfragen abgewickelt.[329] Die End-to-End-Verfügbarkeit des Systems wird mit nahe 100 % angegeben.[330]

Die Kombination der Kreditkarte mit zusätzlichen Dienstleistungen wie Versicherungen oder Bonusprogrammen erhöht den Netzwerkcharakter (im nichttechnologischen Sinne) der Kreditkarten zusätzlich.

Technologisch getrieben fangen die Kreditkartenunternehmen an, nicht nur zur Erhöhung der Sicherheit untereinander, Partnerschaften wie bei SET einzugehen, sondern mit anderen Akteuren zusammenzuarbeiten. Beispielsweise versuchte Visa 2001 mit dem Mobiltelefon-

[324] o.V. (2003g).
[325] o.V. (2003g).
[326] www.mastercardintl.com/newsroom/faqs.html (09.09.2003).
[327] 650 Einwahlknoten weltweit, darunter 13 globale und 32 Länder-Rechenzentren.
[328] Transmission Control Protocol/ Internet Protocol, Standard-Protokoll für Internetzugänge.
[329] www.
[330] o.V. (2003h).

hersteller Nokia und einer Bank, Nordea, ein auf dem Dual-Chip-Ansatz basierendes kreditkartengestütztes mobiles Bezahlverfahren einzuführen.[331]

Die Rückbesinnung auf die Stärke des eigenen Zahlungsnetzes in Kombination mit neuen Technologien lässt den Anbieter Mastercard neue Wege gehen. Unter dem Namen Money-Send soll neben Internet-Zahlungen auch das Mobiltelefon für Zahlungen mit Kreditkarte und Maestro-Karte einsetzbar werden und jeder Kreditkarteninhaber zur Akzeptanzstelle werden.[332] Die Konzeption erlaubt auch internationale Zahlungen von Privat an Privat. Bei 226 Millionen Mastercards und Maestro-Karten in Europa könnten die Finanzinstitute damit die Bemühungen der europäischen Mobiltelefongesellschaften mit deren eigenem Verfahren Simpay ins Leere laufen lassen. Technologisch ist Mastercard beim Bezahlsystem Money-Send in einer aus sicherheitskritischer Sicht günstigen Situation. Die technische Plattform für MoneySend stellt die Paybox-Technologie dar, die sich im Praxisbetrieb als sehr sicher erwiesen hat, und die Anfangsschwierigkeiten, wie z. B. die fehlerfreie Prozessgestaltung trotz Medienbrüchen, überwunden hat.

Einen weiteren Schritt zur Manifestation der Dominanz im Bereich Internet-Zahlsysteme geht MasterCard mit der vorgesehenen flächendeckenden Einführung der Debitkartenzahlung über Debitkarten mit dem Maestro-Symbol. Die technische Lösung sieht vor, eine eWallet (softwarebasierte Brieftasche mit Sicherheitsfunktionalität) auf dem Rechner des Kunden zu installieren.[333] Die technische Anbindung an das Banknetz der kartenausgebenden Bank, bleibt den Finanzinstituten mit deren unterschiedlicher Infrastruktur überlassen. Es bleibt abzuwarten, inwieweit in Deutschland, einem stark Debitkarten-orientierten Land, die Hürde softwarebasierter Installationsvorgänge überwunden werden kann. Gelingt es Maestro, den Installationsprozess dem Kunden zu vermitteln, könnte die Debitkartenzahlung im Internet zu einem neuen Standard werden.

Sicherheit

Die meisten Initiativen, mit denen die Kartengesellschaften zur Zeit in der Presse präsent sind, beschäftigen sich mit der Erhöhung der Sicherheit beim Einkauf mit Kreditkarten. Dies liegt weniger an einer neuen strategischen Ausrichtung, sondern vielmehr an der negativen Presse, denen Kreditkartengesellschaften durch vielfältige und öffentlichkeitswirksame Betrugsfälle immer wieder ausgesetzt sind. In der Folge kam es bei gerichtlichen Auseinandersetzungen zwischen Händlern, Banken, Kreditkartenunternehmen und Konsumenten zu einer, bei der gegebenen technischen Infrastruktur, für die Kreditkartenunternehmen negativen Form der Haftung für einzelne Schadensfälle.[334]

Eine der Möglichkeiten, die zur Erhöhung der Sicherheit diskutiert werden, ist der Einsatz sogenannter virtueller Kreditkartennummern, die beispielsweise bei der O-Card von Orbiscom ohne die reale Kreditkartennummer beim Online-Einkauf auskommen.[335]

Ansonsten sind weltweit zwei geringfügig unterschiedliche Ansätze in der Entwicklung, „Verified by Visa“ und MasterCards „SecureCode“. Beide basieren technologisch konzeptionell auf dem sogenannten 3-Domain-Konzept (3-D), auf dem bereits die SET (Secure Electronic Transaction)-Technologie aufgesetzt hat. Die Kernidee ist es, den reinen Besitz der Kreditkarte und der darauf aufgedruckten Informationen uninteressant zu machen. Erst wer

[331] Vgl. o.V. (2002a).
[332] Vgl. Heise (2003c).
[333] Vgl. www.maestrocard.com/questions/faqs und www.maestrocard.com/internetpurch/ (09.09.2003).
[334] Vgl. ausführlich 5.3.2.1.1.
[335] Vgl. www.orbiscom.com.

im Besitz zusätzlicher Informationen beispielsweise in Form eines Passwortes ist, kann die Karte im Online-Handel einsetzen.

Macht
Die Bedeutung der Kreditkarte weltweit steht außer Frage. Die Unternehmen MasterCard und Visa, im Besitz von Banken und Sparkassen, haben das größte Zahlungssystemnetzwerk der Welt. Ein de facto Monopol, in dem es nur noch zwischen etablierten Kreditkartenorganisationen zum Wettbewerb um Marktanteile kommt. In absehbarer Zeit wird von keinem anderen Anbieter eines Zahlungssystems eine ähnliche Größenordnung erreichbar sein.

Auf dem Markt für Zahlungssysteme im Retailbereich sind die Kreditkartenorganisationen bestenfalls in Nischenmärkten, beispielsweise dem Abrechnen kleinerer Summen im Bereich digitaler Güter und Dienstleistungen, angreifbar. Ansonsten lässt die Erfahrung mit den bisher in Deutschland angetretenen innovativen Zahlungssystemen wie Paybox oder eCash eher vermuten, dass die Kreditkartengesellschaften zwar nicht den „First Mover"-Vorteil für sich werden verbuchen können (und wollen!), aber an den Schwierigkeiten der Mitbewerber ihre strategische Positionierung ausrichten werden, um letztlich mit der Follower-Position sehr gut positioniert zu sein.

Beziehungen zur Aufsicht
Kreditkartenunternehmen unterliegen in Deutschland ebenso dem KWG wie die Geschäftsbanken. Eingebunden in deren Netzwerk sind sie ähnlich positioniert wie die Geschäftsbanken und Sparkassen. Allerdings ist der internationale Aspekt von besonderer Bedeutung; die Aktivitäten der Kreditkartenunternehmen müssen in noch stärkerem Maße weltweit aufsichtskonform sein als lokale Bankgeschäfte oder Zahlungssystemanbieter, die in lediglich einem Land operieren.

4.3.2 (Internet) Payment Service Provider

Zahlungssystemanbieter und -dienstleister sind im Wesentlichen mit dem eCommerce groß geworden. Nach der softwarebasierten Anbindung von Händlern ans Internet sind erst die Payment Service Provider in der Lage, die Zahlungen für die Masse der kleinen und mittleren Händler abzuwickeln, das Clearing vorzunehmen und das Settlement der Zahlung vorzubereiten. Um diese Dienste herum haben sich unterschiedliche Anbieter spezialisiert. Lediglich große Händler wie Otto und Quelle, zumeist bereits vorher im Versandhandel etabliert, betreiben proprietäre Lösungen, die oft auf den klassischen Bezahlverfahren wie der Bezahlung auf Rechnung beruhen. Einzelne „virtuelle" Größen wie der Buch- und Elektronikgerätehändler Amazon und das Online-Auktionshaus eBay folgen ihnen bei diesem Ansatz. eBay ist mit dem Kauf von PayPal allerdings faktisch selbst zum Payment Service Provider avanciert.

Zwei unterschiedliche Ansätze lassen sich unterscheiden, die allerdings in letzter Zeit vermehrt ineinander übergehen. Auf der einen Seite stehen die Entwickler und Anbieter innovativer Bezahlverfahren wie die Firstgate Internet AG, die Paysafecard GmbH und ehemals auch die Paybox AG, die mit ihrem Zahlungssystem auch gleich die notwendigen Zahlungssystem-Dienstleistungen auf dem Markt anbieten. Dazu zählen neben der Bonitätsprüfung der Kunden eines Systems auch Rechnungsstellung, Abrechnung und Marketing- sowie Beratungsdienstleistungen. Auf der anderen Seite gibt es Anbieter, die verschiedene Zahlungsmethoden auf einer Plattform bündeln und den Händlern einen Strauß unterschiedlicher Bezahlsysteme und damit verbundener Dienstleistungen anbieten. Zu letzteren zählen unter anderem die Bibit Internetzahlungen GmbH (mit holländischer Mutter), die Pago eTransactions Services GmbH, als Tochter der Deutschen Bank, Bertelsmann Financial

Services, mit dem Mutterkonzern Bertelsmann AG und Global Collect der TNT Post Group. Nicht alle der genannten Unternehmen sind ausschließlich im Internet Payment-Markt tätig, sondern sind auch im Offline-Handel mit Dienstleistungen rund um den Zahlungsverkehr etabliert.

Die Grenzen beider Anbietertypen können aber auch verschwimmen, etwa mit dem Angebot der Pago eTransactions Services GmbH Online-Überweisungen über das nunmehr eigenentwickelte Verfahren (vormals Stackbox) abzuwickeln.

Spezialisierung
Bisher besteht das Produkt aller (Internet) Payment Service Provider (I)PSP in einem eigenständigen Zahlungssystem und in Dienstleistungen rund um das Bezahlen. Lediglich die Ausprägung der verschiedenen Dienstleistungen variiert, ebenso wie das Preisgefüge für diese Dienste. Es ist nicht abzusehen, dass zusätzliche Dienstleistungen in das Produktportfolio der Payment Service Provider aufgenommen werden.

Technologieführerschaft
Die Akteure in dieser Gruppe bewegen sich naturgemäß alle auf einem technologisch avancierten Feld. Allerdings passen sie sich mit ihren Diensten eher vorhandenen Schnittstellen an als innovative Technologien in besonderem Maße voranzutreiben. In manchen Fällen wie bei der mittelständischen Firma Bibit Internetzahlungen GmbH besteht die Kunst einerseits in der Formulierung der entsprechenden Vertragswerke (schon um dem Verdacht zu entgehen, Bankgeschäfte im Zahlungsverkehr ohne die dazu nötige Banklizenz zu betreiben) andererseits in einer effizienten Gestaltung der Workflows rund um Dutzende von nationalen wie internationalen Zahlungssystemanbietern. Gerade in ihrer Flexibilität und Schnelligkeit und weniger in der Technologieführerschaft liegt die Stärke der Internet Payment Service Provider.

Netzwerk
Auch die Payment Service Provider leben von dem Netzwerk, das sie sich aufbauen. Sie werden vom Endkunden praktisch nicht wahrgenommen, sondern sind ausschließlich auf die Händler und Finanzinstitute und deren Bedürfnisse konzentriert. Die kostengünstige Kombination verschiedener Dienstleistungen, inclusive zugekauften, wie beispielsweise Scoring-Dienste, macht ihre Stärke aus.

Sicherheit
Die Payment Service Provider passen sich ihrem Umfeld an und übernehmen vorhandene Standards, wenn diese vom Markt gefordert werden. So sind beispielsweise die PSPs Partner von Kreditkarteninstituten wie Visa, wenn es darum geht, die neuen Sicherheitslösungen wie „Verified by Visa“ auf der Händlerseite technologisch und prozessorientiert zu implementieren.

Macht
Die Macht der einzelnen Payment Service Provider, den Markt zu beeinflussen und bestimmte Entwicklungen zu gestalten, kann als eher gering eingeschätzt werden. Lediglich die Unternehmen, die über starke Mutterkonzerne verfügen, können indirekt Druck auf den Markt ausüben. Aber gerade die Flexibilität der einzelnen Anbieter macht Abweichungen Einzelner zum Risiko, da die entstehende Lücke im Wettbewerb auch schnell wieder geschlossen werden kann.

Beziehungen zur Aufsicht
Payment Service Provider versuchen durch die entsprechenden Vertragsgestaltungen tatsächlich nur als Dienstleister aufzutreten und nicht in den Verdacht zu kommen, Bankgeschäfte zu betreiben. Damit stehen sie im Zweifelsfall zwar in engem Kontakt zu aufsichtlichen Instanzen, um dieses Ziel zu erreichen. Wenn sie es erreichen, besteht bestenfalls ein indirekter Aufsichts- oder Regulierungsdruck. Die PSPs fallen auch sonst unter keine regulierte Industrie und sind in dieser Hinsicht ungebunden.

4.3.3 Netzwerkbetreiber/Internet Service Provider

Die strategische Position der Telekommunikationsunternehmen wurde durch das UMTS-Debakel, bei dem hohe Ausgaben für den Erwerb von UMTS-Lizenzen und den Netzaufbau entstanden sind, massiv geschwächt. Ansonsten sind diese Unternehmen zusammen mit den Internet Service Providern durch den physischen Aufbau von Netzen und den engen Kontakt zu möglichen Anbietern von Dienstleistungen und zu Kunden prädestiniert, im Bereich Zahlungsverkehr aktiv zu werden. Der Erfolg, den DoKoMo in Japan mit dem Dienst i-mode erzielen konnte[336], ließ die Unternehmen auf ähnliche Erfolge in Europa hoffen, die allerdings bislang ausgeblieben sind.

Spezialisierung
Mit dem Betrieb von Netzen lässt sich in gesättigten Märkten, auf denen kaum noch Neukunden gewonnen werden können, nicht genügend Geld verdienen. So kann erklärt werden, warum die Telekommunikationsunternehmen und Netzwerkbetreiber vermehrt versuchen, Mehrwertdienste zu generieren und zu verkaufen. Dabei bietet sich die Integration einer Abrechnungsmöglichkeit an, da Know-How bei der Rechnungserstellung und Rechnungsversendung in den meisten Fällen bereits vorhanden ist.

Werden über die Netze vermehrt digitale Güter bis hin zu vollständigen Kinofilmen angeboten, müssen diese abgerechnet werden. Verschiedene Ansätze lassen sich erkennen. D2Vodafone und T-Mobile versuchen unter anderem einen Standard für mobiles Bezahlen zu schaffen, mit dem dann auch verschiedene Dienste abgerechnet werden können. Die Deutsche Telekom versucht mit einer eigenen Zahlungssystemplattform, T-Pay, verschiedene Zahlungsmittel zu bündeln und Händlern und Konsumenten eine Auswahl zu ermöglichen.[337] Neben der Telefonrechnung für die Abrechnung von Kleinbeträgen wird die Bezahlung über Micromoney, eine vorausbezahlte Scratchcard, angeboten. Ferner ist die Bezahlung über Kreditkarte aber auch herkömmlich auf Rechnung in T-Pay integriert, weitere Alternativen sind in Planung. Interessant ist diese Dienstleistung für Netzbetreiber, da alle technologischen Voraussetzungen für die Abrechnung beispielsweise digitaler Dienste im UMTS-Netz oder in der GPRS-Vorstufe, von ihnen selbst erfüllt werden können. Das reine „Andocken“ an die bereits existenten Zahlungssystemnetze und -infrastrukturen ist dagegen verhältnismäßig einfach.

An dieser Stelle wird die mögliche Konkurrenz, ähnlich wie bei der von T-Online angebotenen Online-Überweisung, zu den Kreditinstituten offensichtlich. Dabei geschieht die Wertschöpfung nicht über den eigentlichen Bezahlvorgang, sondern über die Marge, die der Händler dem Anbieter einer Zahlungssystem-Plattform bezahlt. Ein weiteres Problem für die Kreditinstitute stellt die enge Einbindung der Netzbetreiber in die Medienlandschaft, und damit zu den potenziellen Anbietern kostenpflichtiger Dienste, dar. Ein Beispiel ist der Erwerb der Fußball-Bundesliga-Rechte durch T-Online für die Gestaltung kostenpflichtiger

[336] Vgl. Krueger (2002), S. 369.
[337] Vgl. TelekomForum (2003).

Dienste, die dem potenziellen Kunden einen Informationsvorsprung liefern, für den er unter Umständen bereit ist, zu bezahlen.[338]

Technologieführerschaft
Aus technischer Sicht gehören die Akteure in dieser Gruppe zu den Anwendern und Vertreibern der innovativsten Technologien und Produkte. Im Gegensatz zu Kreditinstituten, die in diesem Bereich als eher vorsichtig konservativ wahrgenommen werden, möchten die Kunden bei Telekommunikationsunternehmen technologisch auf dem neusten Stand sein und sind durchaus auch bereit, dafür zu bezahlen.

Netzwerk
Telekommunikationsunternehmen und Netzwerkbetreiber sind per definitionem aktiv am Ausbau von Netzen und auch Partnerschaften beteiligt. Diese können im Wesentlichen in zwei Richtungen gehen. Einerseits kann in die Gestaltung kostenpflichtiger Dienste, indem Rechte gekauft werden oder aber im Rahmen von Partnerschaften Dienste auf einer Plattform integriert werden, investiert werden. Andererseits können Finanzdienstleistungen einen höheren Stellenwert erhalten und ausgebaut werden, wie z. B. bei der Online-Überweisung, die T-Online, und nicht eine Bank oder Sparkasse, einem Online-Händler anbietet. Es bleibt abzuwarten, ob das mobile Bezahlen für weitere Impulse sorgen wird, oder ob es letztendlich doch zu strategischen Allianzen von Telekommunikationsunternehmen und Kreditinstituten kommen wird. Zumindest für den Bereich Prepaid-Karten arbeitet die Deutsche Telekom seit Anbeginn mit der Postbank zusammen, die über die nötige Banklizenz für ein solches Geschäft verfügt.

Im Bereich mobiles Bezahlen scheinen die Telekommunikationsunternehmen verstärkt auf Kooperationen innerhalb der Branche zu setzen, beispielsweise mit einer von Vodafone, T-Mobile, Telefonica und Orange gegründeten Allianz für das Bezahlen per Handy. Die Abrechnung soll über die Telefonrechnung oder mit abgesicherter Anbindung über Bankkonto, Kredit- oder Debitkarte erfolgen.[339] Dabei könnten, falls eine gemeinsame Plattform sich durchsetzt, die Netzwerksynergien insbesondere mit den Content-Anbietern aber auch den Entwicklern der passenden Software praktisch ohne Bankenbeteiligung zum Tragen kommen.

Sicherheit
Sicherheit spielt zunehmend auch beim Zugriff auf Daten- und Kommunikationsnetze eine Rolle. Im Bereich Zahlungsverkehr positionieren sich die Telekommunikationsunternehmen mit ihrer unter anderem bereits im Telefonkartengeschäft erworbenen Expertise sehr stark. Die Prepaid-Karten wie die Micromoney-Karte sind technisch vermutlich an der oberen Grenze der Sicherheit angelangt, auch die Produktionsumgebungen sind auf höchstem Sicherheitsniveau. Aber auch der T-Online-Banking Zugang ist bisher kaum negativ in der Presse aufgefallen.

Macht
Im Sinne eines großen Kundenstamms und eines vorhandenen Netzwerkes sind die Telekommunikationsunternehmen gut positioniert. Gleichwohl leiden sie im Hinblick auf die Investitionsfähigkeit noch unter dem UMTS-Problem. Es bleibt abzuwarten, wie sie sich strategisch ausrichten, wenn wieder ausreichende Liquidität verfügbar ist. Zunächst wird es aber gerade bei kostenpflichtigen Diensten notwendig sein, um die nötigen Skaleneffekte zu erzielen, die Kundenbasis durch Kooperationen mit anderen Netzwerkbetreibern und

[338] Vgl. o.V. (2003a).
[339] Vgl. Fluhr (2003), S. 19 und www.simpay.com.

Telekommunikationsunternehmen zu vergrößern. Noch ist allerdings nicht offensichtlich, wie dieser Schritt realisiert werden könnte.

Beziehungen zur Aufsicht
Telekommunikationsunternehmen sind vor allem mit der Deregulierung des Marktes und den daraus resultierenden Problemen beschäftigt. Die Zahlungsverkehrsanwendungen fallen wie im Beispiel der Micromoney-Karte unter die Bankenaufsicht. Da aber in diesem Fall die Postbank als Partnerunternehmen auftritt, werden die aufsichtlichen Belange über diese geregelt.

4.3.4 Dienstleistungsunternehmen

Die Versandhäuser, die im Internet einen idealen zusätzlichen Vertriebskanal entdeckt und entwickelt haben, hätten durchaus einzelnen Internet-Bezahlverfahren zu Akzeptanz- und Wachstumssprüngen verhelfen können – wenn sie auf neue Verfahren angewiesen gewesen wären. Dies war größtenteils nicht der Fall, da die meisten Häuser über Jahrzehnte äußerst valide Datenbanken über ihren wachsenden Kundenstamm aufgebaut hatten, und demzufolge die herkömmlichen Bezahlverfahren bestens bei bekannt geringem Risiko nutzen konnten; beispielsweise die Rechnung bei Erhalt der Ware oder auch die Lastschriftermächtigung. Auf der Umsatzseite scheint diese Strategie aufzugehen. Von 10.000 untersuchten Shops im Internet nutzten 9.950 die Dienste eines Payment Service Providers.[340] Allerdings hatten die restlichen 50 Unternehmen mit eigenen Zahlungssystem-Lösungen einen Umsatzanteil von 90 % der untersuchten Händler! Von dieser Seite kamen nur sehr geringe Impulse, die Entwicklung und den Einsatz neuer Bezahlverfahren voranzutreiben, mit zwei wesentlichen Ausnahmen: Lieferanten digitaler Güter und das Auktionshaus eBay.

Die wachsende Bereitschaft der Konsumenten, für digitale Dienstleistungen und Güter Geld zu bezahlen[341], hat die Grenzen der bestehenden und etablierten Zahlungsverfahren aufgezeigt. Einerseits ist bei sofortiger Lieferung eines digitalen Guts über das Internet die adäquate sofortige Bezahlung beispielsweise per Rechnung (noch) nicht möglich, andererseits sind die Größenordnungen, in denen digitale Güter erworben werden, nicht so groß, dass sich der Einsatz von Verfahren, die ihre Stärken im Macropayment haben, lohnt. Laut Angaben des Verbandes Deutscher Zeitschriftenverleger (VDZ), sind die Nutzer digitaler Dienste durchschnittlich bereit, einen Euro pro Transaktion zu bezahlen.[342] Die Unternehmen, die als Anbieter solcher Dienste auftreten, fordern und fördern geeignete Bezahlverfahren wie beispielsweise die Aggregation von Einzelsummen über die Telefonrechnung der Deutschen Telekom AG oder über Anbieter wie die Firstgate Internet AG.

Beim Online-Auktionshaus eBay ist die Lage etwas anders. Als international agierendes Unternehmen hatte das Haus in den USA größere Probleme, die Bezahlung ersteigerter Güter effizient für Käufer und Verkäufer abzuwickeln. PayPal löste für eBay diese Probleme mit dem Bezahlen über eMail und wurde bis zum Börsengang von eBay kräftig unterstützt und schließlich sogar übernommen. In Deutschland wird der PayPal-Dienst zwar auch angeboten, die anders gelagerte Zahlungsverkehrsinfrastruktur und andere Bezahlgewohnheiten wie die etablierte Überweisung machen diesen Dienst aber für nationale Transaktionen (noch?) nicht sehr attraktiv.

[340] Vgl. Böhle (2002a).
[341] Vgl. Leibold (2003), S. 26f.
[342] Vgl. Heise (2003b), Erhebung basiert auf 12.400 Konsumenten.

Spezialisierung
Die wenigsten Dienstleister diversifizieren ihr Geschäft im Hinblick auf Zahlungssystemdienstleistungen. Sie versuchen vornehmlich, in ihrem Kerngeschäft erfolgreich zu sein. Einzelne Ausnahmen (PayPal von eBay aber auch Global Collect der TNT Post Group) gibt es, bisher bestimmen diese aber in Deutschland nicht den Markt.

Technologieführerschaft
In diesem Geschäft füllen die Dienstleister bisher lediglich von ihnen entdeckte Lücken, die sie mit ihrem eigenen Geschäft überbrücken wollen. Von angestrebter Technologieführerschaft kann keine Rede sein.

Netzwerk
Partnerschaften werden strategisch so ausgerichtet, dass das Kerngeschäft erfolgreich betrieben werden kann. Der Zahlungsverkehr gehört nicht zu diesem Kerngeschäft.

Sicherheit
Die Dienstleister folgen den etablierten Standards und spielen keine weitergehende Rolle bei den folgenden Betrachtungen.

Macht
Die Zahlungssystemdienste sind für die Unternehmen in deren strategischer Ausrichtung von untergeordneter Bedeutung. Die Dienstleister üben somit nur indirekt, über die Bedürfnisse und Ansprüche der eigenen Kunden im Kerngeschäft, Macht auf dem Zahlungsverkehrsmarkt aus.

Beziehungen zur Aufsicht
Aufgrund der untergeordneten Rolle des Zahlungsverkehrs für die Dienstleistungsunternehmen geraten diese in keine besonderen Beziehungen zur Aufsicht. Es sein denn, wie im Fall des Aufkaufens von PayPal durch eBay, sie besitzen als Mutterkonzern ein eigenes Unternehmen in diesem Bereich. Dann fallen sie unter die Rubrik Payment Service Provider.

4.3.5 Verbraucher

Die Verbraucher sind teilweise bei der Entwicklung technologiegetriebener Bezahlverfahren ein wenig aus dem Fokus geraten. Erst als außer der technisch versierten „Early Adopter"-Gruppe keine weiteren Konsumenten und Händler bestimmten Zahlungssystemen ihre Unterstützung gaben, beispielhaft sei eCash der Deutschen Bank genannt, gewannen die Interessen der Verbraucher an Bedeutung.

Seit 1998 werden am Institut für Wirtschaftspolitik und Wirtschaftsforschung, Lehrstuhl Geld und Währung, Prof. Dr. Karl-Heinz Ketterer, regelmäßig Online-Umfragen zum Thema „Internet-Zahlungssysteme aus Sicht der Verbraucher" (IZV) durchgeführt.[343] Neben aktuellen Entwicklungen am Markt für Zahlungssysteme, in jüngster Zeit insbesondere die Abrechnung digitaler Güter und Dienstleistungen, wird bei IZV die Einstellung und die Erfahrung der Verbraucher beim Einkaufen und Bezahlen im Internet systematisch erhoben.

Sicherheit
Zwischen dem Anspruch der jeweiligen Akteure im Zahlungsverkehr, Sicherheit zu erhalten und der Bereitschaft, dafür zu bezahlen, lässt sich eine deutliche Diskrepanz feststellen. Obwohl Plattformen, beispielsweise eBay, „trusted services" anbieten, und die Sparkassenor-

[343] Vgl. u.a. Chakam et al. (2002), Leibold (2003) und www.iww.uni-karlsruhe.de/izv.

ganisation eine eigene Lösung (Treuhand-Bezahlsystem S-ITT) auf dem Markt hat, ist deren Verbreitung gemessen am Online-Umsatz (noch) gering. Im Fall der Online-Auktionen bei eBay kann ein Grund für die geringe Dynamik der Nachfrage an Treuhanddiensten die für den Käufer kostenlose Versicherung[344] sein, die ihn bis zu Werten von 200 Euro bei geringer Eigenbeteiligung vor Betrug schützt.

Sicherheit ist den Akteuren zwar wichtig, jedoch nur im Fall der eindeutig als fehlend wahrgenommenen Sicherheit, lehnen diese den Einsatz der Verfahren deshalb ab. In IZV5 gaben über 60 % der Befragten, die noch kein mobiles Bezahlsystem zur Abrechnung im Internet verwendet hatten, an, dies wegen der von ihnen empfundenen Unsicherheit des Verfahrens nicht getan zu haben.[345] Andererseits zeigt sich die Relativität des Sicherheitsempfindens bei den mobilen Bezahlverfahren: ebenfalls in IZV5 wurden die mobilen Bezahlverfahren von über 90 % der Befragten, die das Prinzip bereits kannten, als sicher empfunden[346]; trotzdem hatten selbst bei denjenigen, die ein solches Verfahren kannten, fast zwei Drittel kein Interesse am Einsatz eines derartigen Verfahrens.[347]

Auch bei der sechsten Umfrage IZV6 im Jahr 2003 gaben die Teilnehmer auf die Frage, warum sie bestimmte Systeme noch nicht benutzt hatten, mit Werten zwischen knapp 15 % (Scratchkarten) bis zu knapp 50 % (Online-Banking), fehlende Sicherheit an.[348] Allerdings wird von noch mehr Verbrauchern als Antwort auf diese Frage die mangelnde Verbreitung der Systeme und die fehlende Gelegenheit, diese einzusetzen, genannt.

Die Subjektivität des Begriffs Sicherheit beim Endverbraucher wird bei IZV6 besonders deutlich. Während bei der Befragung nur 1,9 % der Verbraucher angaben, so schlechte Erfahrungen beim Bezahlen im Internet gemacht zu haben, dass sie in Zukunft auf Einkäufe über dieses Medium verzichten, fühlten sich nur 57,2 % der Befragten sicher, wenn sie im Internet bezahlen.[349]

Macht

Die Position der Verbraucher in Bezug auf Sicherheitsfragen ist relativ stark. Nehmen sie ein Bezahlverfahren gerade aus Angst vor Sicherheitsproblemen nicht an, dann wird dieses Verfahren keinen Erfolg haben. Andererseits zeigt die Online-Umfrage IZV6 auch, dass bei mangelnden Möglichkeiten ein gewünschtes Gut anders zu bezahlen, die Verbraucher auch auf vermeintlich unsicher empfundene Systeme zurückgreifen, seien es Billing- oder Inkassoverfahren oder die Kreditkartenzahlung.[350]

Stärkere Einflüsse dürften von der Seite der Verbraucherorganisationen ausgehen. Wird von diesen ein System oder dessen Sicherheit angeprangert, ist der Aufmerksamkeitsfaktor hoch und der Druck auf die Anbieter, Änderungen anzubringen dementsprechend groß.

4.3.6 Zentralbank/Aufsicht

In Deutschland ist die Deutsche Bundesbank die Zentralbank. Sie ist eingebunden als rechtlich unabhängige Institution in das Europäische System der Zentralbanken. Die

[344] Vgl. www.ebay.de. Der eBay Käuferschutz ist eine freiwillige Leistung von eBay, die ausgesetzt werden kann. 25 Euro werden im Schadensfall als Selbstbeteiligung einbehalten.
[345] Vgl. Chakam et al. (2003), S. 38.
[346] Vgl. Chakam et al. (2003), S. 35.
[347] Vgl. Chakam et al. (2003), S. 38.
[348] Vgl. Leibold (2003), S. 36.
[349] Vgl. Leibold (2003), S. 39 f.
[350] Vgl. Leibold (2003), S. 36.

Europäische Zentralbank (EZB) ist die Kopfstelle des Europäischen Systems der Zentralbanken (ESZB). In den 11 Ländern des Eurosystems gibt es 8.000 Kreditinstitute. Eine der grundlegenden Aufgaben des Eurosystems, und damit der EZB, ist neben der über allem stehenden Gewährleistung der Preisstabilität, das reibungslose Funktionieren der Zahlungssysteme zu fördern. Die EZB agiert dabei vollkommen unabhängig und hat in der Folge einen Haushalt, der nicht Teil des EU-Haushaltes ist (allerdings bestimmen unter anderem die nationalen Zentralbanken über die Höhe des EZB-Haushalts, ein unter machtpolitischen Gesichtspunkten unter Umständen kritischer Aspekt).

Macht
Die Stärke der Institutionen wie BAFin, Deutsche Bundesbank und EZB liegt in der Unabhängigkeit dieser Aufsichtsorgane und Regulierungsinstanzen. Verstärkend wirkt der klare Auftrag, für das reibungslose Funktionieren der Zahlungssysteme Sorge zu tragen. Auf institutioneller Seite sind mit ähnlichen Entscheidungsbefugnissen ansonsten nur noch die EU-Kommission und die Bank für Internationalen Zahlungsausgleich ausgestattet.

In der klaren Definition des Aufgabenbereichs liegt auch die Stärke für den zukünftigen Umgang mit potenziellen Akteuren im Bereich Zahlungsverkehr. Schwieriger ist unter Umständen die Gestaltung des aufsichtlichen Rahmens, wenn vermehrt Akteure aus der Near- oder Nicht-Banken-Welt in den Zahlungsverkehr vordringen. Selbst wenn diese neuen Akteure über Partnerschaften und Allianzen im Zahlungsverkehr aktiv werden, verändert sich das Klima. Unter Umständen müssen neue Prozeduren und Formen der Zusammenarbeit erprobt werden.

Sicherheit
Gerade unter dem Aspekt der Gewährleistung von Sicherheit im Zahlungsverkehr und der dafür notwendigen Regularien und aufsichtlichen Maßnahmen ist das Auftreten neuer Akteure eine Herausforderung. Die zentrale Frage, der auch im Rahmen dieser Arbeit nachgegangen wird, lautet, inwiefern die herkömmlichen Verfahren und Regularien den neuen technologie- und netzwerkgetriebenen Mechanismen gerecht werden.

Der klare Vorteil der aufsichtsführenden Instanzen im Bereich Zahlungsverkehr ist der unstrittige, bereits existierende Auftrag, die Funktionsfähigkeit des Zahlungsverkehrs, und damit indirekt auch die Sicherheit, aufrechtzuerhalten. Die Gestaltung des institutionellen Rahmens bleibt bis auf weiteres bei den bisher dafür bereits zuständigen Institutionen, in jüngster Zeit ergänzt um die EZB.

4.3.7 Strategische Entwicklungsrichtungen

Zusammenfassend lässt sich festhalten, dass der Markt für Zahlungsverkehr und Zahlungsverkehrsdienstleistungen stark in Bewegung geraten ist.[351] Auch wenn das Settlement von Zahlungen weiterhin den Finanzinstituten vorbehalten ist, findet im Bereich der Payment Service Provider und bei deren Produkten und Dienstleistungen ein verstärkter Druck in Richtung Kooperationen mit diesem Akteur statt (siehe Abbildung 14). Einige Akteure, ein Extrembeispiel ist das Online-Auktionshaus eBay, bewegen sich in ihrer strategischen Positionierung auf diese Dienstleister zu, oder kaufen als Mutterkonzern entsprechende Unternehmen auf.

[351] Böhle und Riehm schreiben bereits 1998: „Dem Bankensektor die Beweglichkeit eines Tankers zuzuschreiben, hieße die Dynamik der Kreditwirtschaft zu verkennen – unabhängig davon, inwieweit sie nun als Eigendynamik oder als von außen induziert zu verstehen wäre.“ (Böhle (1998), S. 96).

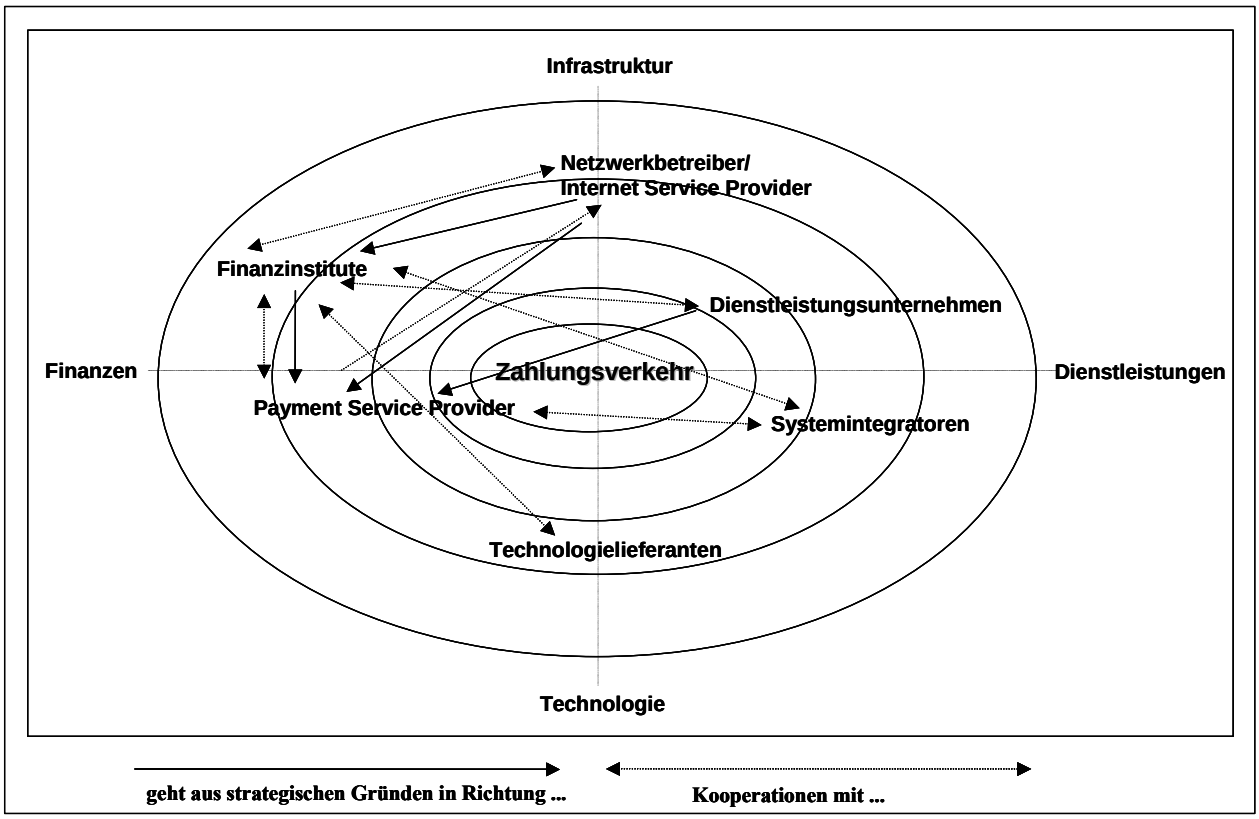

Abbildung 17: Strategische Entwicklungsrichtungen und Kooperationen der Akteure im Zahlungsverkehr[352]

In der Folge entstehen wie bereits beschrieben komplexe Netzwerke. Zu den bereits etablierten Netzwerken der Finanzinstitute, namentlich die Kreditkartennetze, kommen andere Netze, beispielsweise die der Telekommunikationsindustrie, hinzu und vermischen sich. Dies geschieht nicht ohne Reibungsverluste wie insbesondere die schwierigen Kooperationsverhandlungen und auch Zwistigkeiten bei Finanzinstituten und Telekommunikationsunternehmen offenbaren. Der Druck ist an dieser Stelle vermutlich nur kurzfristig durch die Probleme bei der UMTS-Finanzierung und am Aktienmarkt herausgenommen worden. Mit den oben aufgeführten Beispielen zeichnet sich bereits ab, dass neuer Druck bei der strategischen Positionierung aller beteiligten Akteure im Zahlungsverkehr entsteht.

Für die Sicherheit im Zahlungsverkehr und die Rolle der regulierenden Instanzen ändert sich nur auf den ersten Blick recht wenig. Auf den zweiten Blick zeigt sich, dass die Sicherheitskultur, das Regulierungsnetzwerk und die Firmenkulturen ganz Allgemein sich bei den betrachteten strategischen Gruppierungen erheblich unterscheiden. Mit klaren Konsequenzen im Fall vermehrter Kooperationen. Besonders auffällig ist der je nach Branche teilweise unterschiedliche Umgang mit sicherheitskritischen Fragestellungen. An dieser Stelle sei beispielhaft auf die Softwarebranche verwiesen und den seit Jahren schwelenden Streit unterschiedlicher Betriebssystemhersteller um das vermeintlich sicherere System.

In Abbildung 17 wird deutlich, welche Bedeutung der Bezahlvorgang im eCommerce auch aus strategischer Sicht einnimmt.

[352] Eigene Darstellung.

4.4 Sicherheit im elektronischen Zahlungsverkehr: Regulierende Institutionen

Regulierung lässt sich von verschiedenen Seiten klassifizieren. Eine Ebene ist die regionale Bedeutung von Regulierung (international, europäisch/EU, nationale und bankinterne), eine weitere die Unterscheidung in bankspezifische Regulierung und in branchenunspezifische Regulierungen. Eine weitere Möglichkeit ist die Unterscheidung nach Art der Regulierung, z.B. staatliche Regulierung versus private Regulierungsaktivitäten versus Mischformen oder nach Einsatz verschiedener Regulierungsinstrumente.

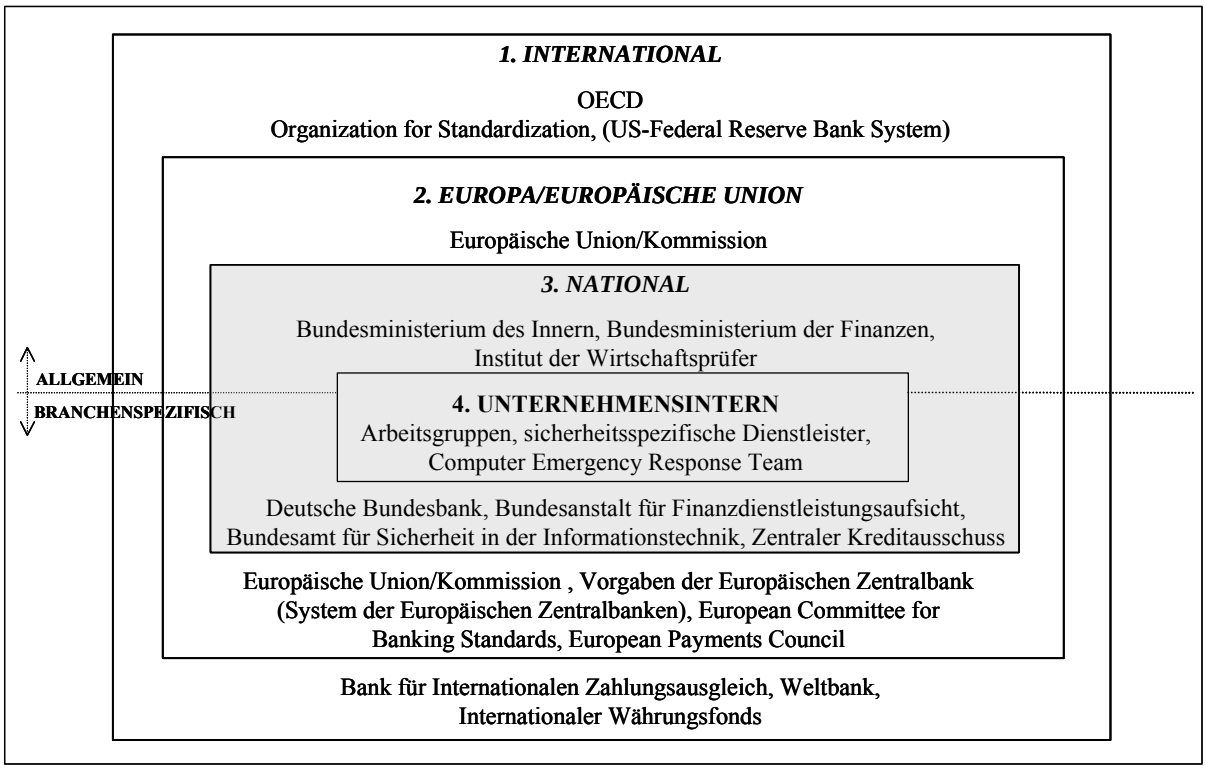

Abbildung 18: Regulierende Institutionen im Bereich „Sicherheit des elektronischen Zahlungsverkehrs“

Kapitel 4.4 ist gemäß Abbildung 18 strukturiert. Es werden regulierende Institutionen ausgehend vom internationalen Umfeld bis auf die nationale Ebene und die Unternehmensebene, die im Zahlungsverkehr und dem Thema Sicherheit eine Rolle spielen können, vorgestellt. Dabei wird zwischen bankenspezifischen Regulierern, unabhängig von ihrer Organisationsform, und allgemeinen branchenunspezifischen regulierenden Institutionen unterschieden.

In Kapitel 4.4 werden zunächst die an der Regulierung des Zahlungsverkehrs direkt oder indirekt beteiligten Institutionen und ihre Rolle bei sicherheitsrelevanten Fragestellungen aufgezeigt. Bei Institutionen, die weniger spezifisch in diesem Bereich tätig sind, gleichwohl in den Kontext gehören, beispielsweise Weltbank und Internationaler Währungsfonds, sind ihre Regulierungsbeiträge und -instrumente bereits in diesem Abschnitt erläutert. Die wesentlichen Beiträge auf nationaler, europäischer und internationaler Ebene werden in Kapitel 5.1 gesondert dargestellt und diskutiert.

4.4.1 Bankenspezifische Regulierer

4.4.1.1 Bankenaufsicht und regulierende Instanzen in Deutschland

Die wesentliche rechtliche Grundlage der Bankenaufsicht in Deutschland stellt das Gesetz über das Kreditwesen (KWG) dar. Die Bankenaufsicht versucht über qualitative und quantitative Rahmenbedingungen, und über die Informationspflicht der Banken der Bankenaufsicht gegenüber, die Funktionsfähigkeit des Finanzsektors zu erhalten, insbesondere im Sinne des Gläubigerschutzes.

4.4.1.1.1 Bundesanstalt für die Finanzdienstleistungsaufsicht

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin), angesiedelt in Frankfurt und Bonn, ist konzeptionell als Allfinanzaufsicht im Mai 2002 aus den ehemaligen Bundesaufsichtsämtern für das Kreditwesen (BAKred), für das Versicherungswesen (BAV) und für den Wertpapierhandel (BAWe) entstanden, mit dem Ziel, dem integrierten Markt für Finanzdienstleistungen durch nur noch einen Ansprechpartner organisatorisch Rechnung zu tragen. Die BAFin ist eine bundesunmittelbare, rechtsfähige Anstalt des öffentlichen Rechts und untersteht der Rechts- und Fachaufsicht des Bundesministerium der Finanzen.

Die BAFin verfolgt als wesentliches Ziel, die Funktionsfähigkeit des gesamten Finanzsektors in Deutschland sicherzustellen. In diesem Rahmen hat die BAFin weitreichende Befugnisse, die von der Einsicht in Bücher, über Sonderprüfungen, Auflagen bis hin zur Schließung einzelner Institute und Handelsplätze gehen.

Für den Zahlungsverkehr sind innerhalb der BAFin die Abteilungen zuständig, die dem ehemaligen Bundesaufsichtsamt für das Kreditwesen (BAKred) zugeordnet waren, daher soll an dieser Stelle kurz die ehemalige Rolle des BAKred erläutert werden.

Das BAKred wurde 1962 in Berlin gegründet und hatte seinen Sitz seit Dezember 2000 in Bonn. Es hatte vor dem Übergang ins BAFin ca. 700 Beschäftigte. Bank- und Finanzdienstleistungsgeschäfte durften in Deutschland nur mit ausdrücklicher Genehmigung des BAKred betrieben werden. Aufgabe des Amtes war und ist heute bei der BAFin die Ausübung der Aufsicht über die Kredit- und Finanzdienstleistungsinstitute in der Bundesrepublik Deutschland.[353] Ziel der Aufsicht ist Risiken und Störungen vorzubeugen, die für die Institute problematisch werden und die Stabilität der Finanzmärkte gefährden könnten.

Grundsätzlich überwacht die BAFin laufend die Arbeit der Institute, unter anderem indem sie die gesetzlich vorgeschriebenen meldepflichtigen Daten auswertet. Zusätzlich kann das Amt Prüfungsberichte durch externe Wirtschaftsprüfer anfordern. Die Machtbefugnisse der Behörde reichen bis zur Durchsetzung der Schließung einzelner Institute bei Verdacht auf Gefährdung der Vermögenswerte der Gläubiger des Instituts. Insbesondere im Zusammenhang mit dem KonTraG ist wesentlich, dass die Behörde auch aufsichtsrechtlich tätig wird, wenn die Organisation der Geschäftsführung eines Kredit- oder Finanzdienstleistungsinstitutes die Sicherheit der Vermögenswerte gefährdende Mängel aufweist oder die ordnungsgemäße Durchführung der Geschäfte nicht mehr gewährleistet ist.

Ein neues Forum für Finanzmarktaufsicht wird im Gesetz über die Bundesanstalt für Finanzdienstleistungsaufsicht (FinDAG) verankert.[354] In diesem Forum sollen neben der BAFin die Deutsche Bundesbank und bei Bedarf das Bundesministerium für Finanzen die

[353] Ungefähr 3.200 Kreditinstitute und 1.200 Finanzdienstleistungsinstitute 2001.
[354] § 3 FinDAG.

aufsichtlichen Belange koordinieren. Mit einem ebenfalls neu zu gründenden Fachbeirat, der 24 Mitglieder aus Finanzwissenschaft, Kredit- und Versicherungswirtschaft, Deutscher Bundesbank und Verbraucherschutzvereinigungen aufweist, soll die BAFin bei der Erfüllung ihrer Aufgaben beraten werden und auch neue praxisrelevante aufsichtliche Themenstellungen diskutieren.[355] Auch im Verwaltungsrat der BAFin ist ein Vertreter der Deutschen Bundesbank, ohne Stimmrecht, vorgesehen. Somit gibt es zwischen den Institutionen Deutsche Bundesbank und BAFin bereits auf der institutionalisierten Ebene einige Querverbindungen, die die Zusammenarbeit positiv beeinflussen können.

Die BAFin ist eingebunden in die Zusammenarbeit mit ausländischen Aufsichtsbehörden. Auf EU-Ebene wirkt sie mit bei dem Ziel der Vereinheitlichung der Aufsichtsvorschriften in der EU. Die BAFin ist u.a. ebenso wie die Deutsche Bundesbank mit einem Sitz im Basler Ausschuss für Bankenaufsicht vertreten.

Eine besondere Konstruktion hat der Gesetzgeber bei der Finanzierung der BAFin, wie auch bereits in den Jahren zuvor bei den anderen in ihr aufgegangen Bundesaufsichtsämtern, gewählt. Die beaufsichtigten Institutionen müssen mit Gebühren und im Umlageverfahren für die Kosten der Aufsicht selbst aufkommen.[356]

4.4.1.1.2 Deutsche Bundesbank

Die Deutsche Bundesbank ist die Zentralbank der Bundesrepublik Deutschland. Das 6. Gesetz zur Änderung des Gesetzes über die Deutsche Bundesbank[357] hat den Veränderungen der dritten Stufe der Europäischen Währungsunion Rechnung getragen. Gemäß § 3 BBankG ist die Bundesbank seit 1999 integraler Bestandteil des Europäischen Systems der Zentralbanken (ESZB) und trägt zur Erfüllung der Ziele mit bei, die für das ESZB definiert sind, unter anderem die Gewährleistung der Preisstabilität aber auch die Sorge um die Abwicklung des Zahlungsverkehrs im Inland und mit dem Ausland und die Sicherung der Stabilität der Zahlungs- und Verrechnungssysteme. Es bleibt festzuhalten, dass die Ziele des ESZB an dieser Stelle faktisch identisch sind mit den Zielen der Bundesbank vor deren Integration in das Eurosystem.

Eine gewisse Eigenständigkeit im internationalen Kontext bewahrt sich die Bundesbank mit § 4 BBankG, der ihr die Zusammenarbeit mit der Bank für Internationalen Zahlungsausgleich und – nach Genehmigung durch die Bundesregierung – weiteren Institutionen gestattet, „die der nationalen Währungspolitik oder dem internationalen Zahlungs- und Kreditverkehr dienen oder sonst geeignet sind, die Erfüllung ihrer Aufgabe zu fördern.“[358]

Das 7. Gesetz zur Änderung des Gesetzes über die Deutsche Bundesbank[359] hat die Organisationsstruktur der Bundesbank im Zuge der Machtverschiebungen innerhalb der Europäischen Währungsunion allerdings stark verändert. Die neue Ebene des ESZB und der Europäischen Zentralbank hat auf nationaler Ebene zu einer de facto Entmachtung der Landeszentralbanken geführt, die nunmehr als Hauptverwaltungen der Deutschen Bundesbank bezeichnet werden und deren weisungsgebundene Präsidenten dem Vorstand der Bundesbank unterstehen.[360]

---

[355] § 8 FinDAG.
[356] §§ 14 – 17 FinDAG.
[357] Verkündet im Bundesgesetzblatt am 30.12.1997.
[358] § 4 BBankG (Beteiligungen).
[359] Verkündet im Bundesgesetzblatt am 28.03.2002.
[360] § 8 BBankG.

Die Bundesbank muss von zwei Seiten betrachtet werden. Einerseits ist sie Organ der Bankenaufsicht in Deutschland. Andererseits ist die Bundesbank selbst Dienstleister im nationalen und internationalen Zahlungsverkehr. In einigen Bereichen „konkurriert“ sie mit ihrem Leistungsangebot dabei mit den Geschäftsbanken und auch mit Zentralbanken anderer Nationen. Dabei wirkt sie als Katalysator zur Gestaltung eines effizienten und sicheren Zahlungsverkehrs.

4.4.1.1.3 Organe der Bankenaufsicht und Zusammenarbeit

Die Bankenaufsicht wird von der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin) ausgeübt. Bei Aufgaben im Kreditwesen arbeitet die BAFin mit der Deutschen Bundesbank zusammen. Im Zahlungsverkehr fungiert die Deutsche Bundesbank unter anderem als Betreiberin von Zahlungssystemen, u.a. von RTGS^{plus} und als Bargeldausgabestelle. Als Aufsichtsorgan übernimmt sie Überwachungs- und Beobachtungsfunktionen und nimmt dabei auch Stellung zu laufenden Entwicklungen in der deutschen Zahlungslandschaft.[361]

Das Aufsichtskonzept gilt als liberal. Der ordnungsrechtliche Rahmen für die innere Struktur und die Geschäftstätigkeit der Kredit- und Finanzdienstleistungsinstitute wird vorgegeben. Die Einflussnahme auf die geschäftspolitischen Entscheidungen der Institute ist jedoch ausgeschlossen. Hoheitliche Aufgaben liegen bei der BAFin, die Bundesbank übernimmt die laufende Überwachung der Kredit- und Finanzdienstleistungsinstitute mit ihrer dezentralen Organisation über die Hauptverwaltungen.

Näher geregelt wird die Aufgabenteilung in § 7 Kreditwesengesetz (KWG) und ausführlich dargelegt in einer Vereinbarung der BAFin und der Deutschen Bundesbank.[362] Die Deutsche Bundesbank übernimmt demnach die laufende Überwachung zu der auch die „Durchführung und Auswertung und der bankgeschäftlichen Prüfungen zur Beurteilung der angemessenen Eigenkapitalausstattung und Risikosteuerungsverfahren der Institute und das Bewerten von Prüfungsfeststellungen“[363] nach § 26 KWG. Sie hat bei dieser Tätigkeit die Richtlinien der BAFin zu beachten; diese werden im Einvernehmen mit der Bundesbank entwickelt und nur im Streitfall wird das Bundesministerium der Finanzen hinzugezogen. Die aufsichtsrechtlichen Maßnahmen wie Verwaltungsakte und Prüfungsanordnungen trifft die BAFin gegenüber den beaufsichtigten Instituten unter Berücksichtigung der Berichte der Deutschen Bundesbank. § 7 Abs. 3-5 verpflichtet die Aufsichtsorgane zum Informationsaustausch, lässt gemeinsame Datenbanken zur Informationsauswertung zu, und macht dementsprechend datenschutzrechtliche Vorgaben.

Die Vereinbarung der Aufsichtsorgane berücksichtigt bereits die laufenden Entwicklungen, die mit Basel II Neuerungen für die Bankenaufsicht mit sich bringen. Die bankgeschäftlichen Systemprüfungen, zu denen Prüfungen nach den Mindestanforderungen an das Betreiben von Handelsgeschäften (MaH) und den Mindestanforderungen an das Kreditgeschäft (MaK) gehören, sollen weiterhin in ähnlichem Umfang von der BAFin beauftragt werden, und je zur Hälfte sollen Prüfer aus der Bundesbank, ergänzt in bestimmten Fällen um Beamte der BAFin, und externe Wirtschaftsprüfer, die von der BAFin bestellt werden, diese Prüfungen

[361] Für Zahlungssysteme ist beispielsweise eine Arbeitsgruppe „Krisenmanagement Zahlungs- und Verrechnungssysteme“ von der Bundesbank etabliert worden, bei der mit den Betreibern der Systeme kritische Themen, z. B. Ausfallplanung im Zahlungsverkehr, diskutiert werden. Allerdings gibt es zur Arbeit dieser und eventueller ähnlicher Arbeitsgruppen keine öffentlich verfügbaren Dokumente.
[362] Vgl. BAFin (2002a).
[363] § 7 KWG Zusammenarbeit mit der Deutschen Bundesbank.

vornehmen. Ein „Beitrittsrecht“ sichert beiden Institutionen zu, bei weiteren Prüfungen der jeweils anderen Organisation eigene Prüfer mit Beobachterstatus zu entsenden.

Neu zu regeln ist einerseits der Umfang der bankgeschäftlichen Prüfungen, die von der BAFin selbst bis Ende 2006, der voraussichtlichen Gültigkeit der Basel II Vereinbarungen, vorgesehen sind, und der Umfang derjenigen Prüfungen, die von der BAFin im Rahmen des mit Basel II eingeführten „Supervisory Review Process“ (SRP) geplant werden.[364] Noch sind die genauen Vorgaben im SRP für die Zentralbanken nicht festgelegt; sicher ist, dass ein kontinuierlicher Überwachungs- und Aufsichtsprozess gerade der Risikosteuerungsverfahren der Institute angestrebt ist, mit Beamten, die laufend vor Ort sind, das heißt bei den Kreditinstituten. Die Federführung für den SRP soll die Bundesbank übernehmen.

4.4.1.1.4 Zentraler Kreditausschuss

Der Zentrale Kreditausschuss (ZKA) wurde 1932 gegründet[365], ursprünglich als Lobbyverein, der politische Willensbildung betreiben sollte. Heute vereint er die fünf Spitzenverbände der deutschen Kreditwirtschaft, den Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V., den Bundesverband deutscher Banken e. V., den Bundesverband Öffentlicher Banken Deutschlands e. V., den Deutschen Sparkassen- und Giroverband e. V. und den Verband deutscher Hypothekenbanken e. V. Die Federführung im ZKA wechselt jährlich zwischen dem Bundesverband der Deutschen Volksbanken und Raiffeisenbanken, dem Bundesverband deutscher Banken sowie dem Deutschen Sparkassen- und Giroverband. Der ZKA betreibt weder eine eigene Geschäftsstelle noch ein Sekretariat mit eigenem Personal, sondern ist beim federführenden Verband an dessen Hauptsitz angesiedelt.

Die Ziele des ZKA sind in zwei Richtungen orientiert. In der Innensicht geht es im Rahmen der geltenden kartellrechtlichen Ausnahmen um die Erarbeitung gemeinsamer Positionen und teilweise auch Strategien in verschiedenen Gremien, wie beispielsweise dem Zentralen Wettbewerbsausschuss.

Nach außen stellt sich der ZKA als gemeinsame Interessenvertretung der kreditwirtschaftlichen Spitzenverbände dar, die eine einheitliche Meinungs- und Willensbildung in bankrechtlichen, bankpolitischen und bankpraktischen Fragen betreibt. Die Bereiche, die im ZKA diskutiert werden, umfassen neben dem Gesellschafts-, Wertpapier- und Steuerrecht und weiterführende Fragen in diesen Fachgebieten auch aufsichtsrechtliche Fragestellungen. Ein wichtiges Aufgabengebiet umfasst die Verhandlung standardisierter Regelungen im Zahlungsverkehr einschließlich der Kartenzahlungssysteme im Rahmen der Zahlungsverkehrsabkommen.

Die Facharbeit des ZKA wird in Arbeitskreisen (oder Arbeitsstäben) und Projektgruppen mit jeweils einem Schwerpunktthema, z. B., Homebanking, geleistet. Vom organisatorischen Charakter her, ohne dass der ZKA ein Organigramm vorhält, sind die Arbeitskreise/-stäbe eher langfristiger Natur und auf dauerhaft aktuelle Themen ausgerichtet, beispielsweise der Arbeitsstab Sicherheitsfragen/-strategie. Projektgruppen sind dagegen schlagkräftige Arbeitsgruppen, die bestimmte relevante Themenfelder bearbeiten, und die nach erfolgreicher Arbeit wieder aufgelöst werden, z. B. die Projektgruppe Signaturprozesse.

[364] Vgl. BAFin (2002a), S. 3., BIZ (2001a).
[365] Vgl. neuer Auftritt des ZKA im Internet unter www.zka.de.

Jeder Verband kann Mitglieder in die Arbeitskreise und Projektgruppen entsenden. Wird dort zu einem Thema ein Konsens gefunden, wird auf der nächsten Ebene eine Vereinbarung verabschiedet, oder wieder in die Arbeitskreise/Projektgruppen zurückverwiesen. Diese greifen bei der Bearbeitung ihrer Themenstellung teilweise auf externes Expertenwissen, beispielsweise von Systemhäusern, zurück. Ein mitunter sehr langwieriger, nicht immer unpolitischer dafür aber umso gründlicherer Prozess, bei dem Fachfragen immer wieder an die dafür zuständigen Experten bis zur endgültigen Klärung zurückverwiesen werden können.

Beschlüsse werden im ZKA einstimmig gefasst und in schriftlichen Stellungnahmen festgehalten. Als Lobbyist vertritt der ZKA die kreditwirtschaftlichen Spitzenverbände gegenüber Behörden, gesetzgebenden Organen, Regierung sowie bank- und finanzwirtschaftlichen Institutionen auf nationaler und europäischer Ebene. Darüber hinaus betreibt der ZKA eine eigenständige Presse- und Öffentlichkeitsarbeit im Sinne der beteiligten Verbände. Dabei ist jeweils der im ZKA federführende Verband für die Adressierung und Veröffentlichung der Stellungnahmen und Pressemitteilungen zuständig.

Ein aus aufsichtsrechtlicher Sicht wichtiger Punkt ist das Freiwilligkeitsprinzip im ZKA. Die Kooperation im ZKA ist nicht durch Gesetz geregelt. Die Beschlüsse des ZKA sind rechtlich nicht bindend, sondern Selbstverpflichtungen der jeweiligen Verbände gegenüber dem Gremium. Allerdings lässt sich im existierenden Geflecht der politischen und geschäftlichen Interessen kaum vorstellen, dass ein Verband aus einer gemeinsamen Position so weit ausschert, dass er die entsprechenden Abkommen oder Beschlüsse konterkarieren würde. Für weitreichende Entscheidungen und die Umsetzung wichtiger Beschlüsse besteht die Möglichkeit der Verpflichtungserklärung, die von den ZKA-Mitgliedern nach Unterschrift als rechtsgültig angesehen wird.

Aus sicherheitstechnischer Sicht ist der ZKA mit seinen spezialisierten Arbeitsstäben und Projektgruppen, beispielsweise dem Arbeitsstab „Sicherheitsfragen/-strategie“ und der Projektgruppe Zulassung (oder Arbeitskreis Sicherheit) ein sehr wirkungsvolles Konstrukt. Der ZKA erarbeitet in den entsprechenden Gremien unter Zuhilfenahme der notwendigen Experten Zulassungs- und Prüfkriterien für Zahlungssysteme oder technische Komponenten, wie beispielsweise die Geldkartenspezifikation (Common Electronic Purse Specification) aber auch hardwarebasierte Vorgaben für die Fertigung von Geldautomaten. Diese Form der Zusammenarbeit bringt notwendigerweise auch Konflikte, die aus den unterschiedlichen Positionen der Mitglieder der Verbände im Wettbewerb resultieren. Klein berichtet im Zusammenhang mit der Einführung des kartengestützten electronic cash-Verfahrens von deutlichen Verzögerungen in der Festlegung technischer Details und von Prüfprozeduren, die nicht unbedingt auf technische Probleme zurückzuführen waren.[366]

Diese Balance zwischen Wettbewerb und Kooperation ist einerseits politisch bedingt durch die kartellrechtlichen Privilegien der Finanzbranche, andererseits zur Gestaltung von Eintrittsbarrieren in den deutschen Bankenmarkt auch von den teilnehmenden Verbänden sicherlich nicht ungewollt. Beispielsweise hat ein Produkt im Zahlungsverkehrsmarkt, das ein Dienstleister den Kreditinstituten anbieten will, sei es ein GeldKarte-Lesegerät oder ein bestimmtes Verfahren zur Online-Überweisung, nur dann eine Chance im Markt, wenn es eine Freigabe vom ZKA – über extern beauftragte Gutachter und unter Umständen die Vorstellung des Produkts vor dem ZKA – erhalten hat.

[366] Vgl. Klein (1997).

Allerdings muss jede Vereinbarung des ZKA mit wettbewerbsrechtlicher Relevanz vom Bundeskartellamt geprüft werden. Während die Festlegung sicherheitskritischer Technologien im aufsichtlichen Sinne sogar erwünscht ist, wird aus wettbewerblicher Sicht im Interesse der Verbraucher versucht, Preisgestaltung im Sinne von gemeinsamen Absprachen zu unterbinden.

4.4.1.1.5 Zusammenarbeit verschiedener Institutionen beim Schwerpunktthema „Sicherheit im eBanking“

In einem Langzeitprojekt sollen die Geldinstitute, die einen Großteil ihrer Geschäfte übers Internet abwickeln, sicherheitstechnisch überprüft werden. Beteiligt sind an diesem Projekt neben der Deutschen Bundesbank die BAFin und das Bundesamt für Sicherheit in der Informationstechnik. Die IT-Infrastruktur wird unter Sicherheitsaspekten einen großen Platz einnehmen. Grundsätzliche Anforderungen an die IT-Sicherheits-Konzeption der Bank sind zu erwarten. Über diese Mindestanforderungen hinaus wird erwartet, dass der IT-Betrieb im Allgemeinen Gegenstand aufsichtlicher Regelungen und Überprüfungen wird. Dabei soll der Netzwerkaufbau, das Betriebssystem, die Schnittstellen zwischen dem e-Banking System und dem Gesamtsystem, die Trennung von Test- und Produktionssystem, die Funktionsfähigkeit der Firewalls und die Reaktion auf externe Angriffe betrachtet werden.[367]

Über die nationalen Aspekte hinaus ist der Basler Ausschuss für Bankenaufsicht seit Jahren bemüht, die besonderen Risiken im elektronischen Geschäftsumfeld zu bewerten und aufsichtsrechtliche Vorschläge zu erarbeiten, die diesen Risiken gerecht werden.[368] Nationale Anstrengungen der letzten Monate versuchen vermehrt, mit den Vorgaben der BIZ koordiniert vorzugehen, da diese im Zweifelsfall auf europäischer Ebene eher Geltung finden als nationale Anstrengungen und im Rahmen der Single European Payment Area konsistenter erscheinen. In diesem Zusammenhang sind die neuesten Veröffentlichungen der BIZ über „Risk Management Principles for Electronic Banking“ und „ Management and Supervision for Cross-Border Electronic Banking Activities“ als Leitfaden für nationale wie europäische Vorgaben zu verstehen.[369]

4.4.1.2 Regulierung des Finanzsektors auf europäischer Ebene

4.4.1.2.1 Europäische Zentralbank

4.4.1.2.1.1 Europäische Zentralbank und Zahlungsverkehr

In Europa ist die Europäische Zentralbank (EZB) eine der jüngsten Institutionen, die durch die Einführung der gemeinsamen europäischen Währung notwendig und durch den Vertrag zur Gründung der Europäischen Gemeinschaft möglich wurde. Vorbereitende institutionelle Arbeiten für die am 1.1.1999 einsetzende Tätigkeit der EZB wurden vom 1.1.1994 bis 31.12.1998 vom Europäischen Währungsinstitut geleistet, das im Gegensatz zur EZB über keine geld- und währungspolitischen Befugnisse verfügte. Zusammen mit den nationalen Zentralbanken der EU-Mitgliedstaaten bildet die EZB das Europäische System der Zentralbanken (ESZB). Die Bezeichnung Eurosystem gilt für die EZB und die nationalen Zentralbanken der Länder, die den Euro bereits eingeführt haben.

[367] Vgl. o.V. (2001).
[368] Vgl. BIZ (1998a), BIZ (2001c), BIZ (2001f), BIZ (2001g).
[369] Vgl. BIZ (2003h) und BIZ (2003i).

Die geldpolitische Verantwortung und die Sorge für einen reibungslosen Ablauf des Zahlungsverkehrs gehören zu den fundamentalen Aufgaben des Eurosystems. Die EZB nimmt bei bankspezifischen Fragestellungen als „Zentralbank der nationalen Zentralbanken" innerhalb der Union und ihrer Gremien eine Schlüsselrolle ein. Der EZB-Rat ist zur Durchsetzung seiner Ziele befugt, Leitlinien und Entscheidungen zu erlassen, bei gleichzeitiger, in den Statuten festgelegter, Unabhängigkeit des Eurosystems von politischen, finanziellen oder personellen Einflüssen.[370] Das Eurosystem ist erst wenige Jahre alt, die Aufgabenverteilung, Machtbefugnisse und detaillierten Verfahrensweisen innerhalb des Systems werden noch diskutiert und sind (noch) nicht frei von nationalen Interessen. Die Prozesse müssen sich einspielen, die EZB kommt zur Feststellung: „Dabei ist es die Aufgabe der EZB und ihrer Beschlussorgane zu entscheiden, wie die Zielvorgaben umgesetzt werden sollen, direkt – d.h. zentral – oder dezentral durch die nationalen Zentralbanken."[371] Als Indikator für die Diskussion im Bereich Zahlungsverkehr können verschiedene „Positionspapiere" der EZB dienen.[372]

Insbesondere Artikel 22 und 34 der ESZB-Satzung geben der EZB im Eurosystem weit reichende Befugnisse für den Zahlungsverkehr.[373] Strukturen, Organisation und Arbeitsschwerpunkte im Zahlungsverkehr des Eurosystems sind noch nicht endgültig ausgeformt. Das ESZB tritt einerseits als wesentlicher Betreiber eines supranationalen Zahlungssystems (TARGET) und andererseits als zuständige Behörde für die Überwachung (engl. supervision) von Zahlungssystemen in Erscheinung; hier gibt es Parallelen zur Deutschen Bundesbank. Die Aufgabe der Aufsicht fällt prinzipiell in den Zuständigkeitsbereich der – bislang noch auf nationaler Ebene angesiedelten – Finanzaufsichtsbehörden. Die Überschneidung von Verantwortlichkeiten, insbesondere zwischen Überwachung und Aufsicht, macht einen ständigen Dialog zwischen den Akteuren erforderlich und institutionelle Veränderungen in Zukunft wahrscheinlich. Bislang gibt es beispielsweise auf europäischer Ebene keine der BAFin entsprechende Institutition, ein Zustand, der unter dem Aspekt des „level playing fields", das heißt einheitlichen Vorgaben für die Unternehmen in allen Nationen der Europäischen Union, überdenkenswert erscheint.

Die EZB ist zwar als Institution jung, ihre Gremien und Komitees jedoch sind vielfach bereits seit Jahrzehnten existent, lediglich deren Bedeutung hat durch die Gründung des ESZB zugenommen. Für aufsichtliche Fragen im Allgemeinen – ohne speziellen Fokus auf den Zahlungsverkehr – spielen zwei Gremien eine herausragende Rolle: das Banking Supervision Committee of the European System of Central Banks und die Groupe de Contact.

4.4.1.2.1.2 Banking Supervision Committee of the European System of Central Banks

Die Gründung des Banking Supervision Committee of the European System of Central Banks (BSC) geht auf das Jahr 1989 zurück. Die Aufgabenbereiche des BSC liegen einerseits bei der koordinierenden Tätigkeit rund um aufsichtliche Fragestellungen im ESZB, andererseits werden generelle Themen, die für die Aufsicht auf nationaler und europäischer Ebene von Interesse sind diskutiert. Dem BSC obliegt es, auf makroökonomischer Ebene Entwicklungen, unter anderem im Zahlungsverkehr, einzuschätzen und diese aus aufsichtlicher Perspektive zu bewerten und gegebenenfalls Maßnahmen einzuleiten.[374]

[370] Vgl. EZB (1999a).
[371] EZB (1999a), S. 59.
[372] Vgl. EZB (2000b), EZB (2002b), EZB (2002e).
[373] Vgl. ausführlich EZB (2002b).
[374] Vgl. KOM (2000b), S. 11ff.

Mitglieder des BSC sind Vertreter der nationalen Zentralbanken und der Europäischen Zentralbank. Beobachterstatus genießen die Europäische Kommission und die Groupe de Contact.

4.4.1.2.2 Groupe de Contact

Die Groupe de Contact/Contact Group (GdC) wurde bereits 1972 bei informellen Treffen des mittleren Managements der europäischen Zentralbanken und Aufsichtsbehörden gegründet, mittlerweile ist die GdC das offizielle Gremium der europäischen Aufsichtsbehörden, die jeweils Mitglieder entsenden. Beobachterstatus haben neben der Europäischen Kommission noch Island, Norwegen und Liechtenstein. Die jeweiligen nationalen Zentralbanken entsenden nur dann Vertreter, wenn sie in ihrem Land aufsichtlichen Pflichten nachkommen. Aus Deutschland nehmen somit ein Vertreter der Deutschen Bundesbank und ein Vetreter der BAFin an den Treffen teil.

Aufgabe der GdC ist es, aufsichtliche Fragestellungen auf mikroökonomischer Ebene zu diskutieren. Es ist das einzige europäische Gremium, in dem gezielt Einzelbetrachtungen aufsichtlicher Fälle durchgeführt werden. Zwar hat das Gremium keine formalen Kompetenzen, jedoch dient es vielfach, da es sehr nah an der täglichen Aufsichtspraxis operiert, als Ideengeber für relevante Themen, die in anderen Gremien wie dem BAC aufgegriffen werden. Das Themengebiet Zahlungsverkehr selbst ist lediglich eines von vielen, die im Bankenumfeld von der Aufsicht diskutiert werden.[375]

4.4.1.2.3 European Payments Council

Die europäische Gemeinschaftswährung und der Druck durch die EU-Preisverordnung[376], die im Kern von den Finanzinstituten eine Angleichung der Gebühren für inländische und innereuropäische Überweisungen (unter bestimmten Voraussetzungen) verlangt, haben die europäischen Organisationen der Finanzinstitute näher zusammenrücken lassen. In der Folge wurde im Sommer 2002 der European Payments Council (EPC) konstituiert. Mitglieder sind die europäischen Bankenverbände, die ebenfalls im European Committee for Banking Standards zusammenarbeiten. Ziel der Arbeit des EPC ist eine mit den Zielen der Single European Payment Area (SEPA) übereinstimmende Zahlungsverkehrsinfrastruktur in die Wege zu leiten, die kostengünstige, sichere und schnelle Zahlungen innerhalb von Europa zulässt.

Der EPC will als europäisches Gremium praktisch aller bedeutenden Finanzinstitute ein Ansprechpartner für das Eurosystem, die Europäische Kommission und das Europäische Parlament sein und entsprechende Vorschläge zur zielgerichteten Einführung der SEPA unterbreiten. Ebenso wie beim European Committee for Banking Standards (ECBS)[377] ist der EPC ein freiwilliger Zusammenschluss zur Selbst-Regulierung der Branche. Die Beschlüsse sind für die Mitglieder nicht rechtlich bindend, allerdings dürfte die gemeinsame Interessenlage hinreichen, um die strategischen Entscheidungen des EPC bei den Mitgliedern umzusetzen.

Organisatorisch ist der EPC von einem sogenannten EPC Plenary geführt, dem ein Sekretariat und eine Koordinierungsgruppe zur Seite stehen.[378] Fünf Arbeitsgruppen in den Bereichen

[375] Vgl. KOM (2000b), S. 14f.
[376] Vgl. Europäische Gemeinschaften (2001).
[377] Vgl. ausführlicher nächster Abschnitt.
[378] Vgl. www.europeanpaymentscouncil.org. Noch finden sich auf den öffentlich zugänglichen Webseiten sehr wenige Informationen.

„Business & Customer Requirements“, „End-to-end Straight Through Processing (STP)“, „Infrastructure“, „Cards“ und „Cash“ mit jeweiligen Unterarbeitsgruppen (Task Forces) stecken die Arbeitsgebiete des Gremiums in Übereinstimmung mit den Zielen des „SEPA White Paper“ ab (siehe Abbildung 19).[379] Auffällig ist, dass das Thema Sicherheit im Zahlungsverkehr keine eigenständige Rolle einnimmt, allerdings beschäftigen sich einzelne Unterarbeitsgruppen mit verschiedenen Aspekten, beispielsweise mit der Betrugssicherheit chipbasierter Karten, den e- und m-Payments und P2P-Aspekten beim STP.

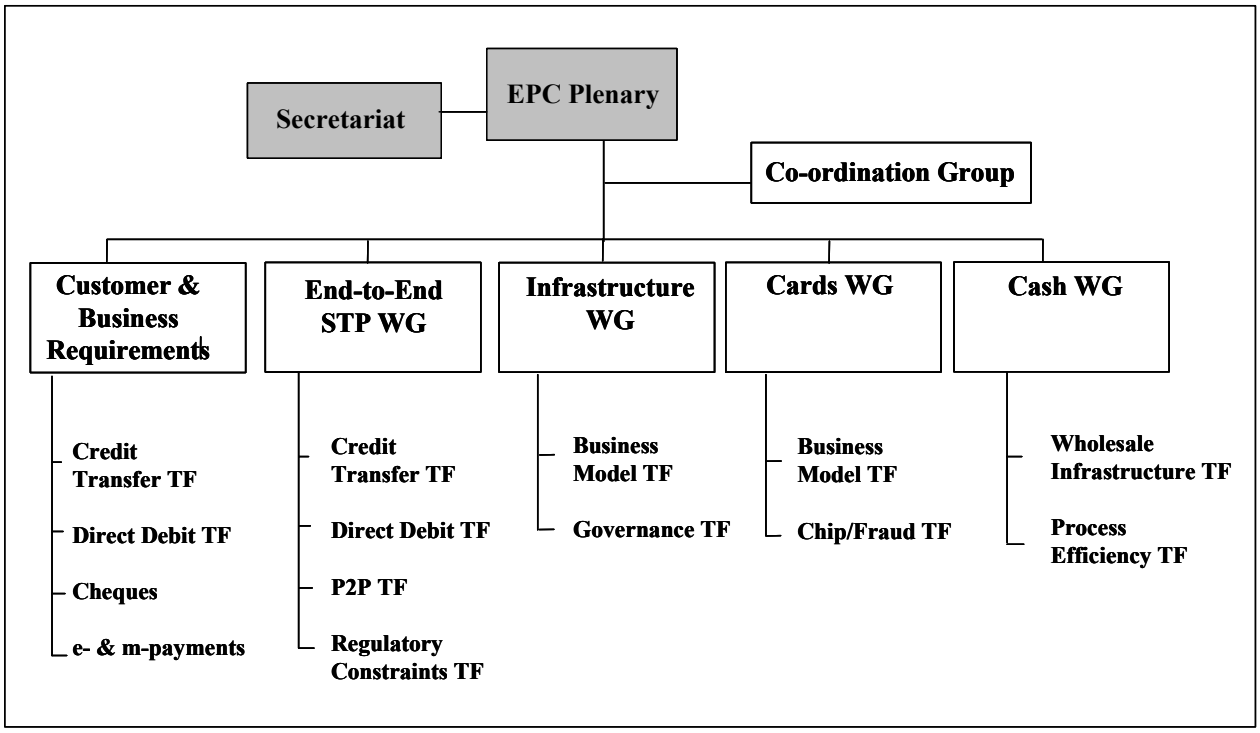

Abbildung 19: EPC-Arbeitsgruppen und Unterarbeitsgruppen[380]

Die Arbeitsgebiete gleichen in einigen Bereichen den bisherigen Arbeiten des ECBS, unter anderem soll bis Juli 2005 ein europäisches Lastschriftverfahren eingeführt werden. Die weiteren Pläne reichen von kurzfristigen Aufgaben wie der Umsetzung der CredEuro-Konvention bis Juli 2003, die die Vorgaben der EU-Preisverordnung umsetzt, über Pläne für ein pan-europäisches Clearinghaus bis Ende 2004 bis zur vollständigen Realisierung der SEPA, und damit der Suche nach neuen Aufgabenfeldern für den EPC, bis Ende 2010.

4.4.1.2.4 European Committee for Banking Standards

Eine regulierend wirkende europäische Nicht-Regierungsorganisation mit Banken als Gründungsmitgliedern findet sich in dem European Committee for Banking Standards (ECBS).[381] Das ECBS arbeitet auf europäischer Ebene dem European Payments Council (EPC) zu. Während der EPC die strategische Ausrichtung der europäischen Bankenlandschaft mitgestalten soll, fällt dem ECBS die Aufgabe zu, die Entwicklung von Standards für das Bezahlen innerhalb der Europäischen Union und soweit möglich darüber hinaus voranzutreiben. Im Selbstverständnis sieht die Organisation ihre Hauptaufgabe darin, „to enhance the

[379] Vgl. EPC (2002).
[380] BdB (2003b), S. 60, Stand Mai 2003.
[381] Vgl. ECBS (2003).

European technical banking infrastructure by developing standards once clear business and commercial interests have been identified“[382]. Im zweiten Teil der Aussage liegt bei widersprüchlichen Interessen ein Problem schneller und zielgerichteter Arbeit. Diese Problematik dürfte auch dazu geführt haben, dass seit 2003 die strategischen Entscheidungen über den Mitte 2002 gegründeten European Payments Council getroffen werden, der direkt mit dem Board kooperiert, welches in Zukunft das ECBS leitet.

Das ECBS ist vorrangig technisch orientiert, die gestalterischen Aufgaben werden vier sogenannten Technical Committees (Payment Cards and Related Devices, Automated Cross Border Payments, Security, Electronic Services) übertragen, die vom Technical Steeering Committee koordiniert werden. Es wird eng mit anderen Standardisierungsorganisationen wie beispielsweise dem European Telecommunciations Standards Institute (ETSI) und der International Organization for Standardization (ISO) zusammengearbeitet.

Gegründet wurde das ECBS Ende 1992 von den drei größten europäischen Organisationen des Finanzsektors (European Credit Sector Associations): Banking Federation of the European Union, European Association of Co-operative Banks und die European Savings Banks Group. Beobachterstatus im ECBS haben neben der Europäischen Zentralbank die Kreditkartenorganisationen, SWIFT und die European Banking Association (EBA).

Ein sichtbarer Erfolg der Arbeit des ECBS ist beispielsweise die europaweite Einführung der International Bank Accounting Number (IBAN), die als Rückgrat einer Single European Payment Area (SEPA) in Europa gelten kann. Die IBAN beinhaltet neben einem Ländercode die Bankleitzahl (oder weltweite Pendants zur Identifizierung einer Bank) und die Konto-nummer sowie mögliche weitere Informationen. Ein anderes Themenfeld, in dem mit der Erstellung technischer Reports (TR 210: Cross Border Direct Debits und TR 211: National Direct Debit Schemes in Europe) Vorarbeiten getätigt wurden, ist die Entwicklung eines einheitlichen europäischen Lastschriftverfahrens.

Ein Technisches Komitee des ECBS ist sicherheitsrelevanten Fragestellungen gewidmet. In bezug auf Zahlungsverkehr beschäftigen sich Publikationen des Gremiums mit sicherem Internet-Banking (1997), dem Risiko, betrügerisch an PINs zu gelangen (1999, TR407 V1) und sicheren Kartenzahlungen über das Internet (2002, TR410 V1). Diese Reports sind teilweise vertraulich.

Analog zur Arbeit des Zentralen Kreditausschusses in Deutschland ist die Einhaltung vereinbarter europäischer Industriestandards für die Mitglieder und Unterzeichner freiwillig – ein Faktum, das sich in Hinblick auf Schnelligkeit und vollständige Marktdurchdringung negativ bemerkbar machen kann.

4.4.1.3 Regulierung des Finanzsektors auf Internationaler Ebene

4.4.1.3.1 Bank für Internationalen Zahlungsausgleich

Die Bank für Internationalen Zahlungsausgleich (BIZ) ist eine internationale Organisation mit Sitz in Basel, gegründet im Jahr 1947. Im Jahr 2001 waren 49 Zentralbanken bei „General Meetings“, den Vollversammlungen, stimmberechtigt. Ziel der BIZ ist, eine koordinierte Zusammenarbeit der Zentralbanken und anderer Organisationen, die die Stabilität des Finanzsystems garantieren, zu gewährleisten.

[382] ECBS (2003), S. 7.

Die BIZ stellt die Infrastruktur für verschiedene Ausschüsse, ständige wie einmalige, die spezielle Fragestellungen rund um Finanzsysteme bearbeiten. Das Committee on the Global Financial System (CGFS) beispielsweise ist für die Beobachtung und das Verständnis der Funktionsweise der internationalen Finanzmärkte zuständig, das Committee on Gold and Foreign Exchange (CGFE) beobachtet die Struktur der Devisenmärkte und beschäftigt sich mit den Implikationen für die Zentralbankpolitiken. Die BIZ ist außerdem Bank der Zentralbanken und bietet diesen Finanzdienstleistungen an. Zusätzlich wird an aktuellen geldpolititschen und monetären Fragestellung in einer eigenen Forschungsgruppe gearbeitet und publiziert. Internationale Abkommen im Finanzsystem werden von der BIZ ausformuliert und nach Konsultationen zur Umsetzung gebracht.

Zusammen mit dem Basler Ausschuss für Bankenaufsicht hat die BIZ das Financial Stability Institute (FSI) 1998 gegründet. Das FSI ist für die Fort- und Weiterbildung von Zentralbankern vorgesehen und soll mit seinen Maßnahmen zur Stabilisierung des Weltfinanzsystems beitragen. Insbesondere soll das FSI helfen, die „Basel Core Principles for Effective Banking Supervision“ in den nationalen Zentralbanken umzusetzen.[383] Eine Ausweitung der Arbeitsgebiete auf die Bereiche Zahlungssysteme und Versicherungen ist vorgesehen. Der Basler Ausschuss für Bankenaufsicht ist zudem federführend bei den Arbeiten zur zweiten Baseler Eigenkapitalvereinbarung (Basel II).

Für Fragestellungen rund um die Effizienz und Stabilität nationaler und grenzüberschreitender Zahlungssysteme ist bisher hauptsächlich der Baseler Ausschuss für Zahlungsverkehrs- und Abrechnungssysteme innerhalb der BIZ zuständig.

Die BIZ ist als internationales Organ empfehlend, koordinierend und vorausschauend tätig, sie hat de jure keinerlei Weisungsbefugnis. Auf der Fachebene jedoch sind die Empfehlungen der Ausschüsse richtungsweisend für die Arbeit der nationalen Zentralbanken und Gesetzgeber. Die supranationalen Netze können nur unter Einhaltung anerkannter Normen und Standards auf nationaler Ebene reibungslos funktionieren. Für die gesetzliche Verankerung sind die nationalen oder im Falle der Europäischen Union die EU-Gremien und EU-Institutionen zuständig. Beispielsweise hat der EZB-Rat 2001 die Grundprinzipien für Zahlungssysteme der G10, ein Resultat der Ausschussarbeit der BIZ, übernommen.

4.4.1.3.1.1 Ausschuss für Zahlungsverkehrs- und Abrechnungssysteme

Der Ausschuss für Zahlungsverkehrs- und Abrechnungssysteme (Committee on Payment and Settlement Systems (CPSS)) ist seit 1990 ein Forum für hochrangige Vertreter der Zentralbanken der Zehnergruppe (G10). Er analysiert die Entwicklungen im Bereich der Zahlungsverkehrs- und Abrechnungsverfahren und untersucht dazugehörige Grundsatzfragen. Der Ausschuss und seine Untergruppen (z. B. die Arbeitsgruppe Massenzahlungsverkehrssysteme) tagen in der Regel bei der Bank für Internationalen Zahlungsausgleich in Basel, Schweiz. Dort befindet sich auch sein ständiges Sekretariat.

Der Ausschuss versucht durch seine Arbeit zur Stabilität des weltweiten Finanzsystems beizutragen. Veröffentlichungen wie die „Core Principles for Systemically Important Payment Systems“[384] tragen zur Standardisierung von Vorgehensweisen im weltweiten Zahlungsverkehr maßgeblich bei. Es handelt sich bei diesen Prinzipien um einen Minimumstandard, der die Stabilität des Weltfinanzsystems aus Sicht der Zahlungssysteme garantiert.

[383] BIZ (1997).
[384] BIZ (2001b eng.).

Systemisch wichtige Zahlungssysteme sind in diesem Fall Interbankensysteme, über die täglich innerhalb der G10 Länder mehrere Trillionen Dollar pro Tag abgewickelt werden, resultierend aus internationalen Finanzgeschäften.

Der Ausschuss veröffentlicht regelmäßig ein „Red Book“ mit statistischen Angaben zu Zahlungssystemen innerhalb der G10 und weiterer kooperierender Länder.

Im Zahlungsverkehr liegt der Fokus des CPSS auf der Analyse, Darstellung und Verbesserung von RGTS-Systemen (Real Time Gross Settlement).

Weitere Arbeitsgruppen im CPSS behandeln Themen rund um Wertpapiertransaktionen, Fremdwährungstransaktionen, Clearing von Derivaten und Zahlungsssystemen. Dabei sind Massenzahlungssysteme in einzelnen Ländern und ihre Settlement- und Clearingpraktiken ebenso Untersuchungsgegenstand wie Entwicklungen rund um elektronisches Geld.

4.4.1.3.1.2 Basler Ausschuss für Bankenaufsicht

Der Basler Ausschuss für Bankenaufsicht (Basle Committee on Banking Supervision (BCBS)) wurde Ende 1974 von den Zentralbankchefs der G10-Länder gegründet. Sein Sekretariat ist bei der BIZ in Basel angesiedelt. Der Ausschuss verfügt über keine formale supranationale Aufsichtsfunktion, seine Empfehlungen und Berichte haben keinen Gesetzescharakter. Trotzdem hat der Ausschuss aufgrund der Mitarbeit der weltweit wichtigsten Zentralbanken (Belgien, Kanada, Frankreich, Deutschland, Italien, Japan, Luxemburg, Niederlande, Spanien, Schweden, Schweiz, GB und USA) eine wegweisende Funktion. Der Basler Ausschuss zeichnet für die Formulierung der Basler Eigenkapitalvorschriften (Basel I) und deren Weiterentwicklung (Neue Basler Eigenkapitalvereinbarung, Basel II) verantwortlich.

Ein Ziel des Ausschusses ist es, über die nationalen Implementierungen der eigenen Arbeiten eine gewisse internationale Konvergenz bei aufsichtlichen Gegebenheiten zu etablieren, ohne politische und institutionelle Zwänge. Der Ausschuss erarbeitet mit seinen ungefähr 30 Technischen Arbeitsgruppen, die sich regelmäßig mehrmals im Jahr treffen, allgemeingültige Standards und Richtlinien sowie „best practices“. Seine „Core Principles for Effective Banking Supervision“ von 1997 und die „Core Principles Methodology“ von 1999 dienen den nationalen Zentralbanken für die Ausarbeitung von Vorgaben, Gesetzesvorlagen und Vereinbarungen der Bankenaufsicht. Dabei sieht sich der Ausschuss selbst in den letzten Jahren verstärkt offensiv auftretend, um sein Ziel, weltweit einheitliche solide Aufsichtsstandards durchzusetzen, zu erreichen.[385]

Eine verstärkte Breitenwirkung der Arbeit des Ausschusses insbesondere auf die nicht aktiv im Ausschuss beteiligten Zentralbanken weltweit soll unter anderem mit der Veranstaltung International Conference on Banking Supervisors (ICBS), die im Zweijahres-Rhythmus abgehalten wird, erreicht werden.

4.4.1.3.2 Internationaler Währungsfonds und Weltbank

Die beiden Organisationen Internationaler Währungsfonds (IWF) und Weltbank sind internationale Institutionen. Beide Organisationen haben 184 Mitgliedsländer und sind „Schwesterinstitute“, die sich in ihrer Arbeit ergänzen sollen.

[385] Vgl. BIZ (2003e).

Bei der Weltbank handelt es sich nicht um eine Bank, sondern um eine Sonderorganisation der Vereinten Nationen. Die Weltbank im engeren Sinne bilden die Internationale Bank für Wiederaufbau und Entwicklung (IBRD) und die Internationale Entwicklungsorganisation (IDA) – ein von der IBRD verwalteter Fonds.[386] Die Ziele der Weltbank liegen vorrangig auf der weltweiten Armutsbekämpfung (u.a. Millennium Development Goals).

Die Ziele des IWF sind deutlicher auf den Zahlungsverkehr und dessen Infrastruktur fokussiert, als dies bei der Weltbank der Fall ist. Artikel 1 der „Articles of Agreement of the International Monetary Fund" nennt als wesentliche Ziele des IWF, um das übergeordnete Ziel des weltweiten Wachstums und Wohlstands zu erreichen, die Förderung internationaler Kooperationen im Bereich Geld und Währung. Dazu zählt neben der Stabilisierung der Währungsbeziehungen auch die Infrastruktur des nationalen wie internationalen Zahlungsverkehrs. Der Betonung der Arbeiten des IWF liegt allerdings auf stabilen Wechselkursbeziehungen (Artikel 4 der Articles of Agreement gibt dem IWF die Möglichkeit die Währungsregime (oder allgemeiner die Finanz- und Geldpolitiken) der Mitgliedsländer zu überwachen („exercise surveillance")[387], die als Grundvoraussetzung für anhaltendes Wachstum gesehen werden.

Der IWF ist auf drei Kerngebieten tätig.[388] Neben technischen Hilfestellungen, die Mitgliedsländern beim Aufbau ihrer Ökonomie gegeben werden, und der dazu notwendigen Vergabe von Kreditlinien, übt der IWF eine Überwachungsfunktion aus. Im Rahmen dieser „Surveillance" des IWF, auch als „Oversight" bezeichnet, wurde 1999 das „Financial Sector Assessment Program" (FSAP)[389] ins Leben gerufen, bei dem Weltbank und IWF gemeinsam den Finanzsektor der Mitgliedsländer untersuchen. Weitere Maßnahmen in diesem Kernfeld der IWF-Tätigkeiten umfassen die Entwicklung und Veröffentlichung von „Best Practices" im Bereich Geld-, Währungs- und Finanzpolitik und die relativ abstrakte Förderung von „Good Governance".

4.4.1.3.3 USA: Federal Reserve System

Grundsätzlich gibt es auf internationaler Ebene im Finanzwesen nur die supranationalen Institutionen, wie beispielsweise die BIZ, Internationaler Währungsfonds oder Weltbank,die regulierend und gestalterisch in das Finanzsystem eingreifen können. Allerdings können auch nationale Vorgaben und Anregungen nationaler Behörden und Institutionen internationale Bedeutung erlangen. Dies ist insbesondere der Fall bei einem ressortübergreifenden Entwurf des amerikanischen Federal Reserve Systems, des Office of the Comptroller of the Currency und der Börsenaufsicht (Securities and Exchange Commission), das unter dem Namen „Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" („White Paper") veröffentlicht wurde.[390] Der Entwurf wurde unter dem Eindruck der Terroranschläge in den USA am 11. September 2001 entwickelt und am 30. August 2002 vorgestellt. Die Fachöffentlichkeit konnte binnen 45 Tagen Stellung nehmen. Die Marktteilnehmer haben den Ansatz überwiegend positiv aufgenommen, teilweise gingen ihnen die Anforderungen nicht weit genug.[391]

---

[386] Weltbank (2003).
[387] IMF (2003a).
[388] Vgl. IMF (2000a), IMF (2003b), IMF (2003c).
[389] Vgl. IMF (2000a), im Detail Abschnitt 5.1.3.2.
[390] Board of Governors (2002)
[391] Vgl. ausführliche Kommentare unter www.sec.gov/rules/concept/s73202.shtml.

Kern der Vorlage ist es, durch verschiedenste Vorgaben, die bis auf die technischen Systeme der betroffenen Institute hinuntergehen können, eine systemische Instabilität des Finanzsektors für Krisen fast jeden Ausmaßes auszuschließen; ausdrücklich solche die regional begrenzt alle dortigen Akteure betreffen könnten. Kritische Systeme sind in diesem Zusammenhang solche, bei denen der Ausfall eines Marktteilnehmers eine Kettenreaktion hervorrufen kann, die aufgrund von resultierenden Liquiditäts-/Kreditproblemen anderer Marktteilnehmer diese ausschaltet. In der vorliegenden Form des Entwurfs wird ausdrücklich nicht der Massenzahlungsverkehr angesprochen, sondern werden ausschließlich Großzahlungssysteme adressiert, ergänzt um Wertpapier- und Devisenhandelssysteme.[392] Der Entwurf fokussiert auf drei Ziele, die in Zukunft im Finanzsektor erreicht werden sollen:[393]

1) Schnelles operatives Funktionieren nach Unterbrechung kritischer Systeme, beispielsweise die Abwicklung noch ausstehender Großbetragszahlungen und das Verarbeiten neuer Aufträge.
2) Schnelles operatives Funkionieren nach größeren Personalverlusten bzw. deren zeitweisem Ausfall.
3) Ein hohes Maß an Sicherheit in Bezug auf tatsächlich im Ernstfall funktionsfähige und umsetzbare Notfallpläne.

Basierend auf den bislang identifizierten Wirkzusammenhängen wurden die „Sound Practices" des White Papers entwickelt und sollen von allen Marktteilnehmern, die systemkritischen Risiken ausgesetzt sind, umgesetzt werden. Wer im einzelnen in die Kategorie „systemkritisch" fällt, ist zum gegenwärtigen Zeitpunkt noch offen, auf jeden Fall die 15-20 größten Banken und die 5-10 größten Wertpapierhandelsgesellschaften in den USA.

Die „Sound Practices" umfassen vier wesentliche Aspekte:

1) Die betroffenen Akteure sollen zunächst alle systemkritischen Aktivitäten identifizieren.
2) Systemkritische Aktivitäten sollen auf jeden Fall noch am gleichen Tag, je nach Bedeutung der Organisation sogar binnen zwei bis vier Stunden nach dem Schadensereignis wieder aufgenommen werden können. Diese Werte sind aus Sicht der Betreiber von Großbetragzahlungssystemen realistisch und vielfach bereits erreicht.[394]
3) In der Folge der zweiten Forderung müssen redundante Systeme außerhalb der Region aufgebaut und vorgehalten werden, die zum einen die Datenverfügbarkeit garantieren, zum anderen genügend Personal entsprechender Qualifikation außerhalb der Schadensregion beinhalten. In welcher Form diese Redundanzen organisatorisch aufgebaut werden, bleibt den Unternehmen überlassen. Klare Vorgaben betreffen die räumliche Trennung der Notfalleinheiten: Diese sollen in Bezug auf die Infrastruktur (Transport, Telekommunikation, Wasser- und Stromversorgung) vollständig von der originären Einheit getrennt sein. Es wird von den Autoren des „White Paper" allerdings betont, dass keine Zersiedelung kritischer Infrastrukturen aus den „Sound Practices" folgt. Die Finanzzentren als solche sollten in ihrer Art fortbestehen.
4) Die Notfallpläne sollen von den Akteuren regelmäßig überprüft werden, insbesondere im Hinblick auf Datenanbindung, Funktionalität und Kapazität. Dies gilt für einzelne Institutionen ebenso wie für das Zusammenspiel der relevanten Akteure im Markt. Dabei wird im amerikanischen Markt unter dem Eindruck des 11.9.2001 betont, dass

[392] Vgl. Board (2002), S. 2.
[393] Board (2002), S. 3.
[394] Vgl. Board (2002). S. 8.

diese Maßnahmen zum festen Bestandteil der Geschäftsprozesse werden sollten und teilweise bereits geworden sind.[395]

Der Zeithorizont für eine eventuelle Anwendung der „Sound Practices to Strengthen the Resilience of the U.S. Financial System" im aufsichtlichen Rahmen ist nicht festgelegt. Ein Vorschlag im Entwurf stellt für die endgültige Umsetzung das Jahr 2007 in den Raum. Allerdings wird erwartet, dass mehrheitlich die Maßnahmen binnen 180 Tagen nach der Veröffentlichung der endgültigen Version des White Paper umgesetzt sein sollten – mit dem Zugeständnis an die Betroffenen, ihre Investionspläne und die Kosteneffizienz der Maßnahmen zu berücksichtigen. Redundante Strukturen außerhalb möglicherweise von einem Schaden betroffener Regionen müssen jedoch noch in 2004 geschaffen werden.[396] Innerhalb der Finanzindustrie wird von unterschiedlichen Ausgangslagen ausgegangen. Während die einen hinsichtlich redundanter Strukturen lediglich am Finetuning arbeiten müssen, fehlen bei anderen sowohl Kapazitäten als auch Humanressourcen, um auf kurze Sicht alle Ziele zu erreichen. Gleichwohl werden die „Sound Practices" nicht in Frage gestellt. Hinsichtlich der Verfügbarkeit von Infrastrukturkomponenten, um den hohen Anforderungen an die zeitnahe Wiederaufnahme kritischer Aktivitäten gerecht zu werden, geht die Industrie von einer rasanten technologischen Weiterentwicklung aus. In der Folge werden aktuell verfügbare „second best" Lösungen eingesetzt, um die Entwicklungszeit zu überbrücken.[397]

Die Tragweite von spezifischen aufsichtlichen Vorgaben in einer großen Volkswirtschaft liegt in der internationalen Verknüpfung der Volkswirtschaften begründet. International tätige Finanzinstitute und Dienstleister würden bei der Anwendung neuer, weitreichender Regelungen unmittelbar betroffen sein und sich bereits im Vorfeld auf solche Entwicklungen vorbereiten müssen, da sie im Ausland in der Regel unter dortiges Aufsichtsrecht fallen. Zwar fällt es einzelnen Nationen durch die Bemühungen zur internationalen Harmonisierung der Bankenaufsicht immer schwieriger, Sonderwege zu gehen; sie können jedoch durchaus – gerade nach Ereignissen wie dem 11. September 2001 – richtungsweisende Impulse für weitergehende Regelungen geben. Insbesondere, wenn diesen Regelungen auf nationaler Ebene höchste Priorität zugestanden wird, wie dies beim „Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" der Fall ist. Noch handelt es sich bei den „Sound Practices" um Empfehlungen der beteiligten Institutionen, es ist allerdings angedacht, diese Empfehlungen in aufsichtliche Vorgaben umzusetzen, sobald die Informationsgüte auf Seiten der aufsichtlichen Instanzen hinreichend hoch ist.[398]

In der veröffentlichten Version des „White Paper" vom August 2002 wird in den Schlussbemerkungen, die vielfach als Fragen formuliert sind, deutlich, dass die beteiligten Behörden noch unklar über die genauen Vorgaben sind, die sie dem Markt nennen sollten.[399] Dies beginnt bei der Festlegung, welche Unternehmen – sogar welche Branche – ab welcher Größenordnung als kritisch zu beurteilen ist und geht weiter zu Detail-Fragestellungen, beispielsweise in welcher Distanz ein Back-up-Zentrum von der Zentrale stehen sollte.

Im „White Paper" wird zusätzlich betont, dass die bisherigen Notfallregelungen, die größtenteils aus der „Jahr 2000"-Umstellung stammen, bei weitem nicht ausreichen.[400] Dies betrifft insbesondere den Aspekt der Vernetzung von Industrieaktivitäten. Während bislang

[395] Vgl. Board (2002), S. 8.
[396] Vgl. Board (2002), S. 6.
[397] Vgl. Board (2002), S. 9.
[398] Vgl. Board (2002), S. 11.
[399] Vgl. Board (2002), S. 11 f.
[400] Vgl. Board (2002), S. 10.

Notfallpläne im eigenen Unternehmen eine Rolle spielten, wird nunmehr diskutiert, die gesamte Prozesskette industrieübergreifend in Notfallpläne zu integrieren. Diese Bemühungen stehen in den USA am Anfang der Entwicklung, werden von der Aufsicht allerdings als notwendiger Schritt zu volkswirtschaftlich relevanten, stabilen (IT)-Gesamtsystemen angesehen.

4.4.2 Regulierung aus dem Nicht-Banken-(IT)-Umfeld

4.4.2.1 Deutschland

4.4.2.1.1 Deutsches Innenministerium und Bundesamt für Sicherheit in der Informationstechnik

Die ökonomische Seite der eGesellschaft wird vom Bundesministerium für Wirtschaft und Arbeit angegangen. Für Fragen der (inneren) Sicherheit im engeren wie im weiteren Sinne ist auf Regierungsebene das Bundesinnenministerium zuständig:[401]

„Der Bundesminister des Innern kümmert sich um die Sicherheit der Bürgerinnen und Bürger in der Informationsgesellschaft. Er sorgt dafür, dass sie den neuen Informations- und Kommunikationstechniken vertrauen können und dass ihre Privatsphäre geschützt bleibt. Jeder Bürger hat das Recht, dass seine persönlichen Daten geschützt werden. Zugleich verlangt die moderne Informationsgesellschaft einen intensiven Datenaustausch. Beide Aspekte müssen in Einklang gebracht werden."

Das Thema Sicherheit in der Informationsgesellschaft wird innerhalb der Bundesregierung vorrangig vom Bundesamt für Sicherheit in der Informationstechnik (BSI) fachlich betreut, eine dem Bundesinnenministerium unterstellte Bundesbehörde.

Die Zuständigkeiten des BSI umfassen dabei:[402]

- „Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen,
- Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten,
- Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten,
- Unterstützung der für die Sicherheit in der Informationstechnik zuständigen Stellen des Bundes,
- Unterstützung der Polizei und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben sowie der Verfassungsschutzbehörden bei der Auswertung und Bewertung von Informationen,
- Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik,
- Beratung auf dem Gebiet des materiellen Geheimschutzes,
- Durchführung von Sicherheitsüberprüfungen von Fernmeldeanlagen einschl. der digitalen Telekommunikationsanlagen bei Bundesbehörden sowie von Unternehmen mit VS-Aufträgen des Bundes."

[401] http://www.bmi.bund.de/frame/dokument/Wir_ueber_uns/Aufgaben_des_BMI/ix3780_18101.htm?script=1, (13.8.2003).
[402] www.bsi.de.

Die Schwerpunktarbeit des BSI liegt unter anderem in den Bereichen Computer-Viren, CERT-Bund, E-Government, Elektronische Signatur, Internet-Sicherheit, IT-Grundschutz und kritische Infrastrukturen. CERT-Bund und E-Government sind dabei die aktuellen Schwerpunkte der Arbeit der Behörde.

4.4.2.1.2 Sicherheitsrelevante Zusammenarbeit in anderen Organisationsformen

4.4.2.1.2.1 Arbeitsgruppe Kritische Infrastrukturen

Die Bundesregierung hat Anfang 1998 eine interministerielle Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) eingesetzt. Die Aufgabe der AG KRITIS liegt darin, „potentielle Bedrohungsszenarien zu bestimmen, über Informationstechnik angreifbare kritische Infrastrukturen auf entsprechende Schwachstellen hin zu prüfen, Möglichkeiten zur Abdichtung solcher Schwachstellen und der Vermeidung oder Minderung eines Schadens zu benennen sowie einen Vorschlag hinsichtlich der Errichtung eines ggf. erforderlichen Frühwarn- und Analysesystems zu erarbeiten.“[403] Als kritische Infrastrukturen werden dabei die folgenden Bereiche gesehen:

- Telekommunikation,
- Transport- und Verkehrswesen,
- Energieversorgung,
- Gesundheitswesen,
- Regierung und öffentliche Verwaltung und
- Bank-, Finanz- und Versicherungswesen.

Die Erkenntnisse sollen veröffentlicht werden. Für den Bereich Kritische Infrastrukturen im Finanzwesen wurde 2002 ein erster Bericht über IT-Sicherheitsinfrastrukturen vom BSI vorgelegt.[404] Wie zu erwarten sind die Beschreibungen der Infrastruktur allerdings so allgemein gehalten, dass ein solcher Bericht nicht zur Anleitung für mögliche Angreifer missbraucht werden kann – die möglicherweise kritischen Informationen blieben unter Verschluss. Da jedoch der Bereich kritische Infrastrukturen in Deutschland traditionell keine besondere Bedeutung hatte und weltweit erst durch den 11.09.2001 wieder an Bedeutung gewonnen hat, sind ähnliche Grundlagenarbeiten für alle als kritisch identifizierten Industrien und Sektoren von großer Bedeutung, um interdisziplinäres Handeln erst zu ermöglichen. In den USA, die im internationalen Vergleich beim Schutz kritischer Infrastrukturen vorne liegen[405], wurde bereits 1996 mit der Einsetzung einer Kommission zum Schutz kritischer Infrastrukturen grundlegende Vorarbeit geleistet, an der sich andere Länder nunmehr orientieren. Unter anderem führte der erste Bericht dieser Kommission in den USA zu einer verstärkten Aufmerksamkeit für das Thema und signifikant erhöhte Investionsausgaben der Regierung für Forschung und Entwicklung im Segment IT-Infrastruktursicherung.[406]

Die mittelfristigen Ziele der AG KRITIS sind hochgesteckt. So soll:

- Eine Bedrohungsanalyse für kritische Infrastrukturbereiche in Deutschland im Hinblick auf ihre IT-Verletzlichkeit erstellt werden.
- Eine IT-Verletzlichkeitsanalyse der für Deutschland wichtigen Infrastrukturbereiche Telekommunikation, Energie und Verkehrswesen durchgeführt werden.

[403] KRITIS (1999), S.6.
[404] Vgl. Münch (2002).
[405] Vgl. Hutter (2002), S. 19.
[406] Vgl. KRITIS (1999), S. 12.

- Der Ausbau und die Fortentwicklung des IT-Grundschutzes speziell für Zwecke des Schutzes kritischer Infrastrukturbereiche vorangetrieben werden.
- Ein Lage- und Informationssystem KRITIS mit technischen und organisatorischen Komponenten konzipiert werden.
- Die KRITIS-orientierte Kooperation zwischen staatlichen und privatwirtschaftlichen Stellen ausgebaut und gefördert werden.
- Die Aufgabe KRITIS beim BSI fortgeführt und ausgebaut werden.

Bedingt durch die hochsensiblen Informationen, die in der AG KRITIS ausgetauscht werden, ist der Stand der verfügbaren Informationen über deren weitere Arbeiten (nach dem Dezember 1999 Papier gibt es keine weiteren öffentlichen Quellen) gering.

Öffentlichkeitswirksam werden zum Thema kritischer Infrastrukturen das BSI und der Arbeitskreis Schutz von Infrastrukturen tätig, unter anderem mit Publikationen und der Durchführung von Tagungen.

4.4.2.1.2.2 Arbeitskreis Schutz von Infrastrukturen

Die Gründung des Arbeitskreises Schutz von Infrastrukturen (AKSIS) erfolgte 1999 auf Initiative des Zentrums für Strategische Studien (ZES). Neben Vertretern öffentlicher Stellen wie Ministerium, BSI, der Polizei und der Bundeswehr sind Vertreter der kritischen Bereiche der Industrie in AKSIS vertreten. AKSIS verfolgt programmatisch das Ziel „die Kritikalität der Abhängigkeiten der Sparten wie Verkehr, Energieversorgung, Banken – und Finanzwesen, Telekommunikation, Sicherheitsdienste und –organisationen, sensitive Wirtschaftsunternehmen und öffentliche Verwaltung von der Informationstechnik und deren Wechselbeziehungen untereinander zu analysieren, darzustellen und Maßnahmen zur Prävention und Reaktion sowie zum übergreifenden Sicherheitsmanagement zu erarbeiten.“[407]

Diese Aufgabenstellung ist nur in enger Kooperation von Industrie und staatlichen Stellen zu erreichen und geht mit dem querschnittsbasierten Ansatz weit über die von den Computer Emergency Response Teams (siehe 4.4.2.1.2.3) verfolgten Ziele hinaus. Dementsprechend sind die Aufgaben von AKSIS zunächst in der Analyse der möglichen Probleme und der Suche nach geeigneten Instrumentarien zum Umgang mit derart komplexen Fragestellungen angesiedelt. Beispielsweise wurde 2001 erstmalig eine Planübung „CYTEX – Cyber Terror Exercise“ durchgeführt, die basierend auf einem Planspiel, Erkenntnisse über die Interdependenzen, Bedrohungspotenziale und mögliche risikomindernde Maßnahmen liefern sollte.[408] Inhaltlich sind sich AKSIS und die AG KRITIS sehr ähnlich.

4.4.2.1.2.3 Computer Emergency Response Centres und Teams

Eine Möglichkeit, den laufenden Herausforderungen durch die Bedrohung von IT-Systemen umzugehen, bietet der Aufbau von Computer Notfall Teams, Computer Emergency Response Teams (CERT) oder Zentren (CERC). Große Unternehmen und auch Finanzinstitute betreiben in der Regel eigene CERTs, auch Computer Security Incident Response Team (CSIRT) genannt, die international operieren können. In Deutschland gibt es nach Angaben der Initiative D21 bislang zehn öffentliche und nicht-öffentliche CERTs; S-CERT ist das einzige CERT, das von Seiten der Finanzinstitute aufgeführt ist – allerdings betreibt beispielsweise

[407] AKSIS (2003), S. 1.
[408] Vgl. CYTEX (2001).

auch die Deutsche Bank AG ein internationales CERT.[409] Von einer flächendeckenden CERT-Infrastruktur, die auch den Mittelstand oder gar Privatnutzer einbindet, kann in Deutschland bislang keine Rede sein. Das Bundeswirtschaftsministerium will gemeinsam mit dem Bundesinnenministerium und der Initiative D21 eine bundesweite CERT-Infrastruktur aufbauen, die insbesondere den Mittelstand unterstützen kann.

Die internationale Dachorganisation der CERTs ist das Forum of Incident Response and Security Teams (FIRST), die mehr als 100 Mitglieds-CERTs betreut.[410] Über FIRST werden per Mailingliste Informationen über Vorfälle, Handlungsempfehlungen und Warnungen ausgetauscht. Allerdings nennt D21 die fehlende tiefergreifende Zusammenarbeit der CERTs als ein Defizit, an dem vorrangig gearbeitet werden müsste.[411]

Zu den Aufgaben eines CERT gehört unter anderem:

- Die Warnung der verantwortlichen Stellen bei möglichen Gefahren, beispielsweise Soft- und Hardwareschwierigkeiten oder Angriffe auf die eigene oder fremde Organisationen
- Sicherheitsanalysen bei Bedarf durchzuführen
- Untersuchung von Zwischenfällen auf ihre Bedeutung
- Koordinierende Funktion bei Zwischenfällen zu übernehmen
- Die Analyse und Nachbereitung von Zwischenfällen
- Forensische Analysen (eigene Durchführung oder Koordination)
- Allgemeine Untersuchungen im IT-Bereich auf Anfrage
- Analyse und Aufzeigen von Schwachstellen (im Auftrag oder präventiv (Qualitätssicherung)

Organisatorisch ist das CERT vor allem mit koordinierenden Aufgaben in die jeweilige Unternehmung (sofern es sich um ein eigenes CERT handelt) eingebunden. Spezialisten werden intern und extern bei Bedarf aktiviert und vom CERT verantworlich geführt.

4.4.2.2 Europäische Union

4.4.2.2.1 Europäische Union und das Thema Zahlungsverkehr

Die Europäische Union ist nicht erst seit der beschlossenen Osterweiterung der EU eine wesentliche (und zunehmende) Quelle regulatorischer Vorgaben. Die Richtlinienkompetenz der EU hat zur Folge, dass nationales Recht sich europäischem Recht anpassen muss. Richtlinien der EU zielen generell auf eine Harmonisierung des Rechtsrahmens und auf einheitliche Wettbewerbsbedingungen. Die Möglichkeit, im Finanzsektor regulatorische Vorgaben in die EU-Mechanismen einzubringen oder voranzutreiben, besteht institutionell innerhalb der Europäischen Union für den Rat der Wirtschafts- und Finanzminister (Ecofin), das Europäische Parlament und die Europäische Kommission.Die Finanzdienstleister werden von diesen Bestimmungen unmittelbar (z. B. Richtlinien zur elektronischen Signatur oder zu E-Geld-Instituten) getroffen. Die Umsetzung in nationales Recht erfolgt innerhalb eines festgesetzten Zeitplans.

Seit den neunziger Jahren, beginnend mit den Vorbereitungen zur Währungsunion, hat die EU das Thema Zahlungsverkehr verstärkt auf die Agenda genommen. Die rechtlichen Vorausset-

[409] Vgl. Initiative D21 (2002), S. 25 f.
[410] Vgl. www.first.org, www.cert.org.
[411] Vgl. Initiative D21 (2002), S. 3.

zungen für die Einführung einer gemeinsamen Währung und die Einrichtung des Eurosystems wurden auf europäischer Ebene gelegt. Die Währungsunion, Anfang 2002 vollzogen, hat das Interesse der Europäischen Union und der Kommission an der Gestaltung des Finanzdienstleistungssektors verstärkt. Das Zusammenwachsen zu einem einheitlichen Wirtschafts- und Währungsraum soll als erklärtes Ziel weiter vorangetrieben werden. Die EU wirkt mit der EZB beispielsweise an der Entwicklung einheitlicher Leistungsvorgaben für den grenzüberschreitenden Zahlungsverkehr mit.[412]

In den letzten Jahren wurde – vor dem Hintergrund der Euroeinführung und der Osterweiterung – im Finanzsektor verstärkt über die Wettbewerbssituation der EU im internationalen Umfeld diskutiert.[413] In der Folge wurde 1998 der Aktionsplan für Finanzdienstleistungen (FSAP) der EU entwickelt, der 1999 in einen Aktionsplan zur Umsetzung des Finanzmarktrahmens für Finanzdienstleistungen mündete.[414] Im FSAP wurden drei übergeordnete strategische Ziele und ein allgemeines Ziel identifiziert, die mit verschiedenen Maßnahmen erreicht werden sollten: 1) ein einheitlicher EU-Wohlesale-Markt, 2) offene und sichere Privatkundenmärkte, 3) moderne Aufsichtsregeln und Überwachung und 4) verbesserte Voraussetzungen für einen optimalen Finanzbinnenmarkt.

Der Zahlungsverkehr nimmt im Rahmen des FSAP keine herausragende Stellung ein, ist jedoch an einigen Stellen explizit genannt, beispielsweise wurde bereits Anfang 2001 der „Aktionsplan der Kommission zur Vorbeugung gegen Betrug und Fälschung“ in Zahlungssystemen umgesetzt.

Jüngste Initiativen der Europäischen Kommission, beispielsweise die Ausrichtung der Konferenz über die Sicherheit von Retail-Bezahlsystemen und das Vertrauen der Konsumenten in Brüssel[415], verdeutlichen, dass die EU-Kommission in diesem Bereich eine gestaltende Rolle einnehmen möchte. Für den Massenzahlungsverkehr ist der Entwurf der Europäischen Kommission „Ein neuer Rechtsrahmen für den Zahlungsverkehr im Binnenmarkt“[416] von entscheidender Bedeutung für die zukünftige regulatorische Ausgestaltung des Zahlungsverkehrs in der Europäischen Union. Die Ausarbeitung eines solchen Rechtsrahmens für den (Massen-)Zahlungsverkehr wird im Neunten Fortschrittsbericht der Europäischen Kommission als Schwerpunkt künftiger Legislativmaßnahmen der Europäischen Kommission gesehen.[417]

Bezüglich der Regelung des (Massen-)Zahlungsverkehrs gibt es nach Auffassung der Europäischen Kommission eine klare Aufgabentrennung zwischen EZB und EU:[418] „Das Privileg der EZB liegt eindeutig im Bereich der Aufsicht über den Zahlungsverkehr und eher technischer Vorschriften zur Sicherheit und Effizienz der Verarbeitung von Zahlungen. Die Aufgabe der Kommission bei Initiativen und Vorschlägen für Rechtsvorschriften zur Regelung der Zahlungsmärkte liegt mehr im Bereich allgemeiner Rahmenregelungen, insbesondere zum Schutz der Nutzer von Zahlungsdienstleistungen.“

4.4.2.2.2 European Commission Banking Advisory Committee

[412] Vgl. KOM (2000a).
[413] Vgl. KOM (2000), Kern (2002), Kern (2003).
[414] Vgl. KOM (1998) und KOM (1999).
[415] Konferenz „Bezahlen & Vertrauen – Wege zur Stärkung der Sicherheit und zum Kampf gegen Risiken“, Europäische Kommission, Brüssel, 16.09.2003.
[416] Vgl. KOM (2003b).
[417] Vgl. KOM (2003a), S. 2.
[418] KOM (2003b), S. 20.

Das European Commission Banking Advisory Committe ((EC)BAC) ist institutionell das zuständige Gremium in der Europäischen Union, um alle aufsichtsrechtliche Fragestellungen im Bankenumfeld zu adressieren. Das BAC hat formal die Aufgabe, die Europäische Kommission fachlich in diesen Belangen zu beraten und bei der Vorbereitung legislativer Initiativen zu unterstützen. Die Legitimation für seine Arbeit bezieht das BAC von der First Banking Co-ordination Directive (77/78/EWG), in dem die Gründung, der Status als beratendes Organ der Kommission und die Aufgabenbereiche des BAC festgelegt sind.[419]

Das BAC selbst hat keine Funktion als „Regulierer", wird an dieser Stelle jedoch aufgeführt, da die Kompetenz für sämtliche aufsichtlichen Fragen rund um den Bankensektor auf EU-Ebene in diesem seit 1978 bestehenden Gremium institutionalisiert wurde. Die Zusammensetzung des BAC geht über die Aufsichtorgane (Bankenaufsicht der Länder) hinaus; es partizipieren ebenso die Finanzministerien und die Europäische Kommission. Beobachterstatus haben die Europäische Zentralbank und Norwegen, Island und Liechtenstein.

Der Aufgabenbereich des BAC ist sehr weit gefasst, Zahlungsverkehr zählt nicht zu den Kernkompetenzen des Gremiums. Von Bedeutung ist der BAC vor allem, da es eines der wenigen Gremien auf EU-Ebene sein dürfte, das umfassend über die aufsichtlichen Positionen der Mitgliedsländer zu einzelnen Fragestellungen informiert ist. Insofern ist das BAC ein idealer Ansprechpartner, sollte wie geplant der EPC seine Arbeit intensivieren und sich zu einem europäischen ZKA entwickeln.

4.4.2.3 International

4.4.2.3.1 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

Auf internationaler Ebene gibt es keine staatliche Organisation oder Institution, die verbindliche Vorgaben in speziellen Branchen oder branchenübergreifend in Bezug auf (IT)-Sicherheitsvorgaben macht. Einen sehr weiten Rahmen spannt die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD).[420] Als Zusammenschluss von 30 führenden Industrienationen sieht die OECD ihre Aufgabe im Vorantreiben wichtiger gesellschaftlicher und ökonomischer Prozesse, die den Wohlstand erhöhen könnten. Aus Sicht der OECD spielt dabei die Informationsgesellschaft eine wichtige Rolle, die Rede ist von der „global information society" (GIS), und eCommerce bietet darin ein gewaltiges Potenzial wirtschaftlicher Entwicklung.

Für Sicherheitsbelange der Informationsgesellschaft ist innerhalb der OECD die „Working Party on Information Security and Privacy" (WPISP) zuständig. Die WPIPS „promotes an internationally coordinated approach to policymaking in security and protection of privacy and personal data in order to help build trust in the GIS and facilitate electronic commerce."

Die WPISP sieht sich als international agierender Vermittler zwischen staatlichen Stellen, die bisher für die Sicherheit gesellschaftlich bedeutender Infrastrukturen zuständig waren, und der Industrie, die in der Informationsgesellschaft auf der Infrastrukturseite eine bedeutende Rolle spielt. Ziel der Arbeit der OECD ist neben der Förderung des Dialogs beteiligter Akteure, eine erhöhte Wahrnehmung für das Thema Sicherheit und eTrust bei allen zu erreichen und zu helfen, Richtlinien zu entwickeln, wie die Sicherheit und Privatsphäre in offenen Netzen geschützt werden kann. Die Richtlinien werden über Jahre hinweg immer wieder aktualisiert und neuen Begebenheiten angepasst.

[419] Vgl. KOM (2000b), S. 5ff.
[420] Vgl. www.oecd.org.

Die wesentlichen Arbeiten der OECD in diesem Bereich umfassen die „OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data“ von 1980 und die aus dem Jahr 1997 stammenden „OECD Guidelines for Cryptography Policy“. Ein Beispiel für die verhältnismäßig abstrakt und allgemein gehaltene Arbeit der OECD sind die „OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security“.[421] Die Richtlinien verfolgen das Ziel, das Thema Sicherheit der Informationstechnologie gesellschaftlich und kulturell zu verankern, das Vertrauen der Akteure in die Informationstechnologie zu erhöhen, und Standardisierungsbemühungen voranzutreiben.[422] Um diese Ziele zu erreichen werden neun ineinander greifende Grundprinzipien entwickelt, die das Bewusstsein der Marktteilnehmer für Sicherheit stärken sollen, Verantwortlichkeiten festlegen und Maßnahmen vorschlagen (Risk-Assessment-Prozeduren, Security Design, Security Management, Reassessment etc.). Auf dieser abstrakten Ebene werden ferner in zwei Grundsätzen ethische Fragestellungen und demokratische Prinzipien behandelt.

Der OECD-Rat ist sich der begrenzten Möglichkeiten der Richtlinien durchaus bewusst und formuliert in der Veröffentlichung einschränkend:[423] „...the *Guidelines* [...] set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations; And recognising that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security.”

4.4.2.3.2 International Organization for Standardization und International Electrotechnical Commission

Die International Organization for Standardization (ISO) mit Sitz (Sekretariat) in Genf ist die größte Organisation ihrer Art. In der ISO, einer Nicht-Regierungsorganisation, sind 147 nationale Standardisierunginstitute vereint. Die Mitglieder sind je nach nationaler Struktur private oder staatliche Organisationen. Auf dem Gebiet der Informationstechnologie arbeitet ISO mit der International Electrotechnical Commission (IEC), ebenfalls mit Sekretariat in Genf, eng zusammen.[424] 1986 wurde zu diesem Zweck das ISO/IEC Joint Technical Committee 1 (JTC1) gegründet, in dem IT-Standards entwickelt und veröffentlicht werden.[425]

Bei der ISO/IEC-Standardisierung handelt es sich um Vorschläge, die von der Industrie auf Basis der Freiwilligkeit übernommen werden können. Teilweise finden diese Normen Eingang in hoheitliche regulatorische Vorgaben, teilweise ermöglicht erst die Einhaltung der Standards neue Produkte und Dienste. Die Grundidee der Standardisierungsarbeit ist, von Anfang an Experten aus der Industrie in den entsprechenden Technischen Kommitees, Arbeitsgruppen etc. zu haben, so dass die Arbeit praxisgetrieben bleibt. Weltweit arbeiten für ISO ca. 30.000 Experten, bei ISO/IEC JCT1 sind es 2.100. Seit der Gründung der ISO im Jahr 1947 wurden ca. 13.700 Standards veröffentlicht, im Bereich ISO/IEC JCT1 kommen jährlich zwischen 100 und 150 IT-Standards hinzu.

[421] OECD (2002a). In der ersten Fassung bereits 1992 veröffentlicht.
[422] Vgl. OECD (2002a), S. 8f.
[423] OECD (2002a), S. 14.
[424] Vgl. www.iec.ch.
[425] Vgl. www.jtc1.org.

5 Operationelles Risikomanagement und Regulierungsinstrumente im elektronischen Zahlungsverkehr

Es gibt für die Sicherheit im elektronischen Zahlungsverkehr potenziell eine Vielzahl von regulierenden Institutionen mit einem breit gestreuten Instrumentarium.

In Kapitel 5.1 werden zunächst die diversen Regelungen im Bereich Banken im Hinblick auf den Zahlungsverkehr in ihrer Bedeutung für die Sicherheit der Systeme aufgezeigt. Die Betreiber von Zahlungssystemen, sowohl von Retailsystemen als auch von Großbetragszahlungssystemen, werden in ihrem Risikomanagement mit diesen Regelungen, Vorschriften und Gesetzestexten konfrontiert.

In Kapitel 5.2 wird dargelegt, welche Grundüberlegungen und Vorgehensweise in allgemeiner Hinsicht für das Risikomanagement existieren. Die branchenunspezifischen Ansätze des Risikomanagements werden betrachtet und ihre Grenzen aufgezeigt.

Es zeigt sich, dass für den Zahlungsverkehr das Management Operationeller Risiken im Rahmen der Basel II-Verhandlungen von besonderer Bedeutung wird. Ausgehend von dieser Erkenntnis werden in Kapitel 5.3 die regulatorischen Vorgaben und Ansätze der Basel II-Vereinbarungen ausführlich dargestellt und ihre Bedeutung für den elektronischen Zahlungsverkehr diskutiert. Anhand der aufgezeigten Grenzen des aktuell in Basel II diskutierten Ansatzes wird abschließend ein weiterführender Vorschlag präsentiert, der auf den bereits erzielten Erfolgen im Basel II-Prozedere aufsetzt.

5.1 Instrumente der Regulierer: (IT-Security-) Regelungen im Bankenwesen unter besonderer Berücksichtigung des elektronischen Zahlungsverkehrs

Ausgehend von den in Kapitel 4 identifizierten Akteuren, die für die Festlegung und Durchsetzung von Regularien im elektronischen Zahlungsverkehr verantwortlich sind, werden im folgenden Abschnitt die für die Sicherheit in der Informationstechnologie geltenden Bestimmungen dargestellt und auf ihre Relevanz hin untersucht. In Abbildung 20 werden die wesentlichen Regelungen nach regionaler Herkunft und Bezug aufgeführt. Es können im Wesentlichen internationale, europäische und nationale Regelungsebenen unterschieden werden, ergänzt um eine unternehmensinterne Komponente. Von Bedeutung ist ferner der Adressatenkreis der Regelungen. Vereinfachend wird dabei zwischen allgemeinen und branchenspezifischen Ansätzen unterschieden. Idealerweise sollten dabei die branchenspezifischen Regularien detailliertere Vorgaben beinhalten als allgemeine Regelungen, die keine Branchenspezifika berücksichtigen können.

Es gibt verschiedenste Instrumente für eine zielgerichtete Regulierung. Für den Bereich Zahlungsverkehr sind in Tabelle 3 die bedeutendsten Ausprägungen aufgeführt und mit Beispielen unterlegt. Dabei ist im Hinblick auf die Durchschlagskraft diese Tabelle im Wesentlichen von oben nach unten zu lesen, das heißt für Europa, dass EU-Rechtsverordnungen einen bindenden Charakter für alle Marktteilnehmer der Europäischen Union haben, während „best practices“ oder Notfallpläne in der Regel unternehmensintern angewendet werden und nur dort bindend sind, bzw. überprüft werden. Vereinbarungen auf freiwilliger Basis, d.h. ohne staatlich regulativen Druck, etwa die im ZKA beschlossenen Zahlungsverkehrsabkommen, hängen in punkto Durchsetzbarkeit von der Reputation des Gremiums ab, in dem sie verhandelt werden. Je größer die gegenseitigen Abhängigkeiten – beispielsweise von gemeinsamen Datenformaten, die gegenseitig anerkannt werden – umso weniger können sich einzelne Institute aus dem vereinbarten Rahmen heraus bewegen.

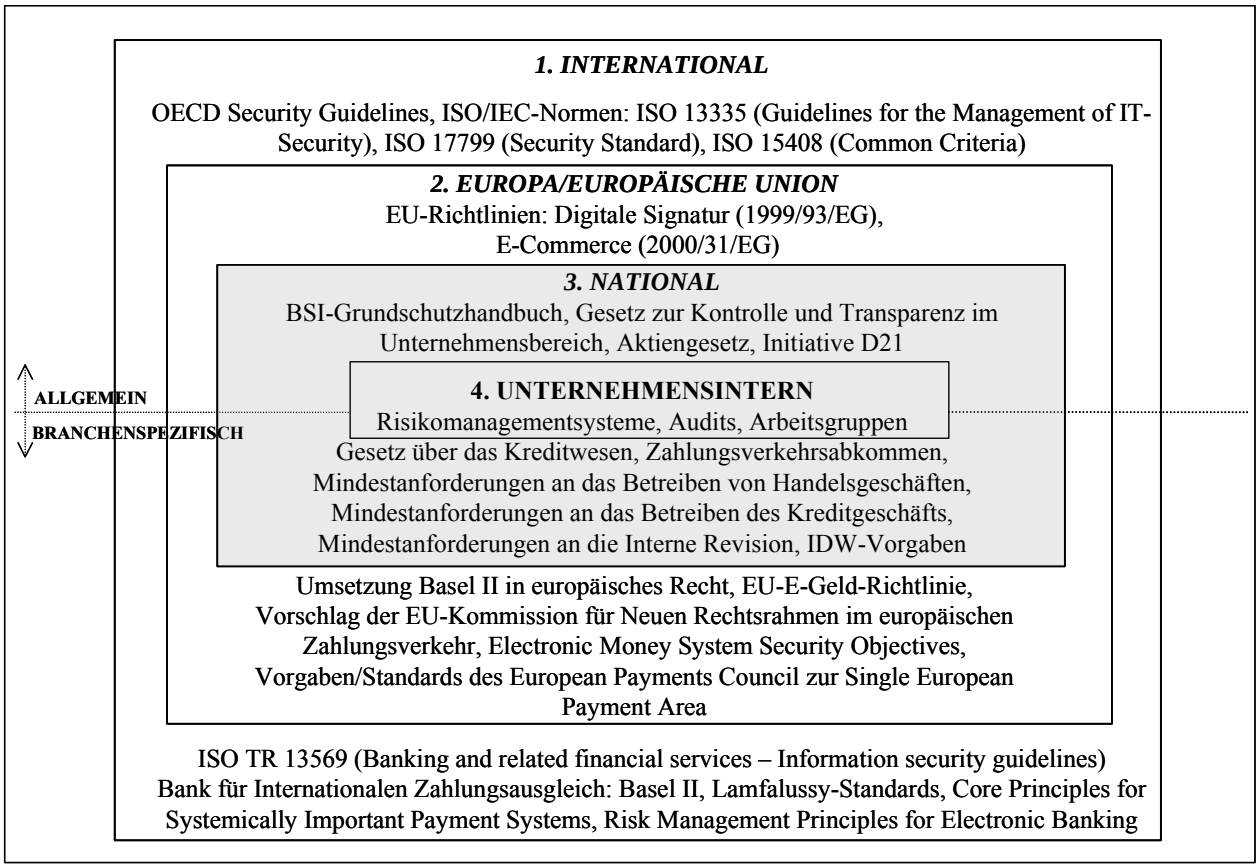

Abbildung 20: Regulierung unter Bezug auf Sicherheit auf internationaler, europäischer und nationaler Ebene

Unter dem Gesichtspunkt der aufsichtlichen Überprüfung von existierenden Regelwerken können die in Tabelle 4 aufgeführten Ausprägungen regulatorischer und aufsichtlicher Tätigkeiten unterschieden werden. Dabei ist besonders auf den Unterschied zwischen Aufsicht und Überwachung hinzuweisen. In Europa versteht sich die Europäische Zentralbank im Zahlungsverkehr primär als Organ der systemischen Überwachung (oversight) und Marktüberwachung (surveillance), während die Aufsichtsfunktion auf nationaler Ebene (prudential supervision) in Deutschland von der Bundesanstalt für Finanzdienstleistungsaufsicht in Einvernehmen mit der Deutschen Bundesbank ausgeübt wird. Ein supranationales Aufsichtsorgan, ein europäisches Pendant zur BAFin, fehlt in Europa bislang. Die Diskussionen um die Reform der EU-Regulierungs- und Aufsichtstrukturen, die mit dem Aktionsplan für Finanzdienstleistungen (FSAP) vorangetrieben wird, zeigen den Bedarf nach eine gemeinsamen Regulierungs- und Aufsichtsbehörde auf EU-Ebene (European Financial Services Authority) deutlich. Es steht die Forderung im Raum, eine solche Institution zumindest im Rahmen einer Ermächtigungsklausel in den neu auszuhandelnden EU-Verträgen vorzusehen.[426]

[426] Vgl. Kern (2003), S. 11.

Deutsche Bezeichnung	Englische Bezeichnung	Beispiele
EU-(Rechts-)Verordungen	EU-regulations	Verordnung über grenzüberschreitende Zahlungen in Euro (2560/2001/EG)
Richtlinien, Direktiven	directives	Richtlinien über E-Geld (2000/46/EG und 2000/28/EG)
(Nationale) Gesetze	laws	Kreditwesengesetz
EU-Entscheidungen und EU-Beschlüsse	EU-decisions	Rahmenbeschluss über Betrug im Zusammenhang mit unbaren Zahlungsmitteln
Standards	standards	ISO 17799 Information Security Management
Schreiben/Verlautbarungen		17-Punkte-Schreiben des BAKred zur grenzüberschreitenden Datenfernverarbeitung im Bankbuchführungswesen
Grundsätze, Grundregeln	principles	Grundprinzipien für Zahlungsverkehrssysteme, die für die Stabilität des Finanzsystems bedeutsam sind
Leitlinien	guidelines	OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security
(Zahlungsverkehrs)-Abkommen	(technical) agreement	ZKA-Zahlungsverkehrsabkommen
Vertragswerke/Regularien	rules, agreement	Verträge/Regularien der Kreditkartenorganisationen
Empfehlungen	recommendations	Empfehlung der Kommission über elektronische Zahlungsinstrumente (97/489/EG)
Vorbilder	best practices/ sound practices	Sound Practices for the Management and Supervision of Operational Risk
Notfallplanung	contingency planning	Regelungen einzelner Institute

Tabelle 3: Instrumente der Regulierung (nach abnehmender rechtlicher Bindungskraft sortiert)[427]

Es kann gezeigt werden, dass die neueren Institutionen im Bereich Zahlungsverkehr, beispielsweise die Europäische Zentralbank, bislang neben der systemischen Überwachung vornehmlich eine Beobachterrolle (observation, monitoring) einnehmen – wenngleich die EZB de jure insbesondere bei Marktversagen weitreichende Befugnisse hat.

Die Prozesse der Steuerung und Prüfung sowie des Melde- und Berichtswesens sind einerseits auf unternehmensinterne Vorgänge bezogen, andererseits für die vorgeschriebenen Auskünfte gegenüber den Instanzen der Aufsicht und der (Markt)überwachung notwendig.

[427] Hartmann (2003) mit eigenen Ergänzungen.

Aufsicht	**(prudential) supervision**
Überwachung (systemisch)	**oversight**
Marktüberwachung	**surveillance**
Beobachtung	**observation, monitoring**
Steuerung, Prüfung	**control, check**
Melde- und Berichtswesen	**reporting**

Tabelle 4: Funktionalitäten der Regulierung – Ausprägungen der aufsichtlichen Umsetzung[428]

Aus institutioneller Sicht bleibt die Frage nach einer effizienten Zuordnung der Tätigkeiten ‚Aufsicht', ‚Überwachung (systemisch)' und ‚Marktüberwachung' offen. Während sich in Deutschland eine historisch bedingte Rollenaufteilung ergeben hat, besteht auf europäischer Ebene die Chance, eine Zuordnung der jeweiligen Aufsichtstätigkeit zur geeigneten Institution unter Effizienzkriterien durchzuführen. Ein erster Ansatz hierzu wird in Kapitel 6 vorgestellt.

5.1.1 Regelungen in Deutschland

5.1.1.1 Gesetz über das Kreditwesen

Das Gesetz über das Kreditwesen (KWG) ist die wesentliche juristische Säule der Bankenaufsicht in Deutschland. Es wird regelmäßig durch Novellen an aktuelle Entwicklungen angepasst. Zuletzt wurden im Zuge der Zusammenfassung der Aufsichtsämter zur BAFin mit dem Gesetz über die integrierte Finanzdienstleistungsaufsicht[429] die notwendigen Anpassungen der Aufsichtsorgane in den Gesetzestexten (BAFin statt BAKred etc.) geregelt.

Für den Anwendungsbereich des Gesetzes über das Kreditwesen (KWG) gilt, dass alle Unternehmen, die Bankgeschäfte betreiben (incl. Netzgeld- und Geldkartengeschäft) dem KWG unterliegen. Das KWG fokussiert in den meisten Paragraphen auf die kaufmännischen Grundlagen, Bestimmungen und Meldevorschriften für Bankgeschäfte. Seit der 6. Novelle des KWG 1997 nimmt die Funktionssicherung des Zahlungsverkehrs als Aufsichtszweck mehr Raum ein, insbesondere das Geldkarten- und Netzgeldgeschäft (§1 I 2 Nr. 9, 10 und 11 KWG) soll in die Überwachung einbezogen werden.

Unter dem besonderen Blickwinkel der IT-Sicherheit im Bankensektor kann der in der 6. Novelle des KWG neueingefügte § 25 a ‚Besondere organisatorische Pflichten von Instituten' als bedeutend betrachtet werden. In Absatz 1 Abschnitt 1 heißt es, dass ein Institut über geeignete Regelungen zur Steuerung, Überwachung und Kontrolle der Risiken sowie über angemessene Regelungen verfügen muss, anhand derer sich die finanzielle Lage des Instituts jederzeit mit hinreichender Genauigkeit bestimmen läßt. In Absatz 1 Abschnitt 2 wird ferner gefordert, dass ein Institut über eine ordnungsgemäße Geschäftsorganisation, ein angemessenes Kontrollverfahren sowie über angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung verfügen muß.

Somit wird in diesen beiden Abschnitten die grundlegende Forderung nach einem funktionierenden Risikomanagement niedergelegt. Die dazugehörige Aufzeichnungs- und Dokumenta-

[428] Hartmann (2003), getrennte Darstellung.
[429] Vgl. IntFinDAG (2002).

tionspflicht wird in Absatz 1, Abschnitt 3 festgeschrieben: Ein Institut muss dafür Sorge tragen, dass die Aufzeichnungen über die ausgeführten Geschäfte eine lückenlose Überwachung durch die BAFin für seinen Zuständigkeitsbereich gewährleisten; die erforderlichen Aufzeichnungen sind sechs Jahre aufzubewahren; § 257 Abs. 3 und 5 des Handelsgesetzbuches gelten entsprechend.

Für Outsourcing-Maßnahmen, als klassisches Beispiel IT-Maßnahmen, gilt zusätzlich KWG § 25 a Absatz 2. Demnach darf bei einer Auslagerung von Bereichen auf ein anderes Unternehmen, die für die Durchführung der Bankgeschäfte oder Finanzdienstleistungen wesentlich sind, weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen noch die Steuerungs- oder Kontrollmöglichkeiten der Geschäftsleitung, noch die Prüfungsrechte und Kontrollmöglichkeiten der Bundesanstalt beeinträchtigt werden. Das Institut hat sich insbesondere die erforderlichen Weisungsbefugnisse vertraglich zu sichern und die ausgelagerten Bereiche in seine internen Kontrollverfahren einzubeziehen. Das Institut hat die Absicht der Auslagerung sowie deren Vollzug der BAFin und der Deutschen Bundesbank unverzüglich anzuzeigen.

Auffallend an der Formulierung in § 25 a ist die für Gesetze übliche weitgefasste Formulierung, die in Begriffen wie „angemessenen" Kontrollverfahren oder Sicherheitsvorkehrungen zum Ausdruck kommt. Allerdings fehlt die sonst übliche Präzisierung durch Verordnungen oder Prüfnormen in diesem Fall bislang vollständig. Damit wird als Folge politischer Entscheidung beim Gesetzgebungsverfahren den Finanzinstituten die alleinige Verantwortung für ihre geschäftspolitischen Entscheidungen überlassen. Es erfolgt kein direkter Eingriff in einzelne Geschäfte der Institute durch die Bankenaufsicht.

5.1.1.2 Mindestanforderungen der Bundesanstalt für Finanzdienstleistungsaufsicht

Die BAFin ist in den letzten Jahren den Weg zu qualitativen Vorgaben im Bereich des Risikomanagements auf allen Kreditinstitutsebenen sehr konsequent gegangen. Die Schwierigkeiten flexibler Regelungen mit Öffnungsklauseln werden dabei bewusst in Kauf genommen, um auf die Markterfordernisse, die Weiterentwicklungen auf dem Gebiet des Risikomanagements und auf internationale Regulierungen wie Basel II angemessen reagieren zu können. Von Bedeutung für den Zahlungsverkehr sind die Mindestanforderungen nicht direkt. Wichtig sind sie, da einerseits der Wandel im aufsichtlichen Verständnis hin zu einem flexibleren Umgang mit den Kreditinstituten zum Ausdruck kommt, andererseits die geforderte Risikomanagementumgebung für den Umgang mit Operationellen Risiken, und damit auch dem Zahlungsverkehr, maßgeblich ist.

5.1.1.2.1 Mindestanforderungen an das Betreiben von Handelsgeschäften

Die Mindestanforderungen an das Betreiben von Handelsgeschäften (MaH) haben ursächlich keinen Zusammenhang mit Bezahlsystemen. Gleichwohl stellen sie einen schon frühzeitig 1995 gesetzten Standard für den Umgang mit Risiken bei Handelsgeschäften und damit auch Operationellen Risiken dar.

Grundsätzlich wird in den MaH ein Risikocontrollingsystem zur Messung von Risiken und ein Risikomanagement zum Handling dieser Risiken gefordert. Die Anforderungen an das System sind qualitativer Natur, es soll flexibel sein und möglichst in die Gesamtrisikosteuerung der Kreditinstitute einzupassen sein. Diese Auffassung wird im Rundschreiben 4/98 des BAKred verstärkt, es „wird kein bestimmtes Verfahren oder Modell für das Risiko-

Controlling und -Management vorgegeben."[430] Allerdings müssen die Systeme dem Risiko angemessen sein, eine Anforderung, die schwierig zu objektivieren ist.

In den MaH wird beispielsweise gefordert, Geschäfte mit neuartigen Produkten oder neuen Märkten gesonderten Risikokontrollen zu unterziehen und es werden Anforderungen an das Risikomanagement gestellt, die explizit Operationelle Risiken, z. B. rechtliche Risiken und Betriebsrisiken sowie eine angemessene technische Ausstattung, berücksichtigen.[431] Ohne auf deren genaue Ausgestaltung einzugehen, erhält die technische Infrastruktur in den Bestimmungen der MaH eine besondere Gewichtung: Veränderungen bei den EDV-Systemen sind Teil der Berichtspflicht bei Revisionen.

5.1.1.2.2 Mindestanforderungen an das Betreiben des Kreditgeschäfts

Die Mindestanforderungen an das Betreiben des Kreditgeschäfts (MaK) stellen eine Konkretisierung – wenngleich mit vielen Öffnungsklauseln, um der Verschiedenartigkeit der Kreditinstitute zu entsprechen – des § 25 a Abs. 1 KWG dar, der eine angemessene Risikomanagementstruktur fordert. Sie sind de facto eine Vorstufe der Anforderungen, die durch Basel II auf die Institute zukommen. Dies gilt inhaltlich für den Umgang mit Kreditrisiken, deren Management in Basel II international harmonisiert wird, und zeitlich, da der Zeitpunkt für die schlussendliche Implementierung der MaK in den Kreditinstituten zum 31.12.2005 mit dem Wirksamwerden der Basel II Anforderungen ab 2006 zusammenfällt.[432]

Die Umsetzung der MaK soll stufenweise erfolgen. In der ersten Stufe soll bis zum 30.6.2004 die Aufbauorganisation dokumentiert sein, zum 31.12.2005 sollen die IT-bezogenen Anforderungen umgesetzt sein. Bereits Ende 2003 ist der Stand der Implementierung in der Jahresabschlussprüfung zu dokumentieren und in den Folgejahren soll über die Umsetzung der Stufen 1 und 2 berichtet werden.[433]

Das Rundschreiben 34/2002 der BAFin zu den MaK vom 20.12.2002 legt neben den allgemeinen Anforderungen fest, wie die Organisation des Kreditgeschäfts zukünftig ausgestaltet sein muss, welche Risikoklassifizierungsverfahren angewendet werden können, und wie die Identifizierung, Steuerung und Überwachung von Risiken im Kreditgeschäft gestaltet sein muss. Daneben sind Fragen der Auslagerung und der Prüfungen durch Revisionen und Abschlussprüfer abgehandelt.[434]

Für die Sicherheitsfragen der Zahlungssysteme spielen die MaK eine untergeordnete Rolle, da sie sich auf Kreditrisiken beziehen. Von Bedeutung werden die MaK wegen des Verständnis der Aufsichtsorgane in Bezug auf Risikomanagementprozeduren und den flexiblen Umgang mit verbesserten Techniken.

In einzelnen Punkten sind die Anforderungen an das Management der Kreditrisiken sehr nah an dem von Basel II vorgesehenen Umgang mit Operationellen Risiken. Beispielsweise wird von der BAFin gefordert, vor der Aufnahme neuer Produkte und Geschäftsarten ins Portfolio oder dem Markteintritt auf neuen Märkten zunächst umfassende Risikoprüfungen vorzunehmen.[435] Diese gehen über „klassische" Kreditrisiken hinaus in die Operationellen Risiken

[430] BAKred (1998), S.1.
[431] Vgl. BAKred (1995), Abschnitt 2.3.
[432] Vgl. BAFin (2002b), S. 4.
[433] Vgl. BAFin (2002b).
[434] Vgl. BAFin (2002c).
[435] Vgl. BAFin (2002c), Tz. 18f.

hinein. Dazu zählen unter anderem bei solchen Neuentwicklungen die Berücksichtigung von personellen, organisatorischen, rechtlichen und datenverarbeitungstechnischen Konsequenzen, unter Hinzunahme verschiedener Instanzen von der Geschäftsleitung bis zur Revision. Die Analogie zu den bereits 1995 etablierten MaH ist unverkennbar.[436]

Weitere Schnittstellen zu einem Management Operationeller Risiken ziehen sich durch das gesamte Rundschreiben. So wird für die geforderte Funktionstrennung bei der Vergabeentscheidung von Krediten eine informationstechnologische Unterlegung dieser Trennung gefordert. Kann diese von den Anwendern umgangen werden, liegt ein klares Operationelles Risiko vor. Prozesse bei der Kreditvergabe müssen in Zukunft auf ihr Kreditrisikogehalt hin ausgelegt werden – eine ähnliche Vorgabe findet sich in den „Sound Practices for the Management and Supervision of Operational Risk" ebenfalls. Auch die geforderten Kreditrisikoindikatoren, bei denen gesonderte Prozesse, z. B. Problemkreditbehandlung, initiiert werden müssen, finden ihre Analogie bei den Operationellen Risiken und dort zu definierenden Frühwarnindikatoren. Wie bei den Operationellen Risiken findet sich bei den Kreditrisiken die Problematik der Quantifizierung von Risiken wieder: Neben den quantitativen Elementen sollen verstärkt auch qualitative Kriterien berücksichtigt werden.[437]

Besonders deutlich wird die Bedeutung der MaK als Vorstufe der Umsetzung von Basel II bei der geforderten Identifizierung, Steuerung und Überwachung der Risiken im Kreditgeschäft.[438] Allerdings bleiben die MaK wie auch im Begleitschreiben der BAFin angekündigt[439] bei der Methodenwahl offener als die Basel II Ansätze, die verschiedene Verfahren und Klassifizierungen zur Auswahl vorschlagen. Die implizite Betonung der Rechts- und Betriebsrisiken[440] verdeutlicht den engen Zusammenhang und die Schwierigkeit der Abgrenzung von Kreditrisiken und Operationellen Risiken. Eine unzureichende technisch organisatorische Ausstattung der IT-Systeme beispielsweise ist ein typisches Operationelles Risiko und nicht zwingend ein Kreditrisiko. Gerade diese Querbeziehungen bei einzelnen Risiken betonen die Notwendigkeit eines kontrollierten Gesamtrisikosteuerungsprozesses, der im Rundschreiben 34/2002 gefordert wird.[441]

5.1.1.2.3 Mindestanforderungen an die Interne Revision

Das BAKred hat die Mindestanforderungen an die Ausgestaltung der Internen Revision der Kreditinstitute(MaIR), die noch aus dem Jahr 1976 datierten, in seinem Rundschreiben 1/2000 aktualisiert.[442] Grundsätzlich basieren die MaIR auf § 25 a Abs. 1 Nr. 2 KWG. Dort werden eine ordnungsgemäße Geschäftsorganisation und angemessene interne Kontrollverfahren bei Kreditinstituten erwartet.

Die Interne Revision hat alle Betriebs- und Geschäftsabläufe eines Unternehmens je nach Risikogehalt zu überprüfen. Insbesondere ist auch die Anwendung, Funktionsfähigkeit, Wirksamkeit und Angemessenheit der institutseigenen Risikomanagement- und Risikocontrollingsysteme zu prüfen und zu beurteilen. Dabei hat die Interne Revision weitreichende Befugnisse im Hinblick auf ihr zustehende Informationen aus dem Unternehmen, eigene

[436] Vgl. BAKred (1995), Abschnitt 2.3, zum Zusammenspiel der einzelnen Regelungen vgl. Deutsche Bundesbank (2003b).
[437] Vgl. BAFin (2002c), Tz. 70. Ausführlich zur Schwierigkeit qualitativer versus quantitativer Normen vgl. 6.2.2.
[438] Vgl. BAFin (2002c), Abschnitt 6.
[439] Vgl. BAFin (2002b).
[440] Vgl. BAFin (2002c), Abschnitt 6.5.
[441] Vgl. BAFin (2002c), Tz. 73.
[442] Vgl. BAKred (2000b).

qualifizierte Personalressourcen müssen zur Verfügung stehen, und die Unabhängigkeit darf nicht gefährdet werden. Die Überprüfung der Arbeit der Internen Revision obliegt dem Abschlussprüfer gemäß Prüfungsberichtsverordnung.

Im Hinblick auf Operationelle Risiken wird die Interne Revision aller Voraussicht nach eine wichtige Rolle bei der Beurteilung der eingesetzten Risikomanagementsysteme erhalten. Noch ist allerdings nicht absehbar, ob die qualitativen Vorgaben beispielsweise der „Sound Practices of the Management and the Supervision of Operational Risk" der BIZ für eine Prüfungsgrundlage ausreichen. Wird in weiterführenden Rundschreiben eine klare Überprübarkeit der Anforderungen sichergestellt, könnte die Interne Revision eine Organisationseinheit sein, die der Aufsicht bei der Beurteilung der institutsinternen Verfahren in weiten Teilen zuarbeitet.

5.1.1.3 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist am 1. Mai 1998 in Kraft getreten. Das Gesetz verfolgt zwei grundsätzliche Regelungsziele. Einerseits soll das Kontrollsystem des deutschen Aktienrechts verbessert werden und andererseits sollen die deutschen Publikumsgesellschaften besser den internationalen Kapitalmärkten und ihren Bedürfnissen nach Informationen Rechnung tragen.[443]

Für die IT-Security auch bei Banken ist der durch das KonTraG eingefügte neue § 91 Abs. 2 Aktiengesetz (AktG) wesentlich. Der Vorstand hat demnach geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, welches den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkennen läßt (Risikofrüherkennungssystem). Die Verpflichtung des Vorstands, eine Gesellschaft verantwortlich im Sinne der Eigentümer zu leiten, bestand bereits vor der Gesetzesänderung. Das KonTraG betont diese Notwendigkeit zusätzlich und erleichtert die Geltendmachung von Schadensersatzansprüchen gegenüber Vorstandsmitgliedern, die ihre Pflichten gemäß AktG und KonTraG verletzt haben.

Das KonTraG fordert ein Überwachungssystem, mit welchem Maßnahmen zur Erfassung und Kommunikation von Risiken in geeigneter Weise umgesetzt werden können. In § 317 HGB Abs. 2 Satz 2 wird dies noch verstärkt: „... dabei ist auch zu prüfen, ob die Risiken der zukünftigen Entwicklung zutreffend dargestellt sind." In § 317 HGB Abs. 4 wird bei der Rechtsform der Aktiengesellschaft für die Abschlußprüfung gefordert, zu beurteilen, „ob der Vorstand die ihm nach § 91 Abs. 2 des AktG obliegenden Maßnahmen in geeigneter Form getroffen hat, und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann." Dazu zählt auch die in § 289 Abs. 1 neu eingefügte Forderung „... dabei ist auch auf die Risiken der zukünftigen Entwicklung einzugehen."[444]

5.1.1.4 Wirtschaftsprüfer: Vorgaben durch Grundsätze und Prüfungsstandards

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) ist ein freiwilliger Zusammenschluss von Wirtschaftsprüfern und –prüfungsgesellschaften. Der IDW ist einerseits eine Interessenvertretung der Wirtschaftsprüfer, andererseits wird vom IDW Standardisierungsarbeit geleistet, indem nach mehreren Review-Prozessen und öffentlicher Diskussion durch Fachausschüsse Prüfungsstandards (IDW PS), Standards (IDW S), Stellungnahmen zur

[443] Zur Bedeutung vgl. KPMG (1998). Bei dem Gesetz handelt es sich um ein sogenanntes Ergänzungs- und Änderungsgesetz, d.h. es ist kein eigenständiges Gesetz, sondern verändert und ergänzt bestehende Gesetze wie beispielsweise das Aktiengesetz.
[444] Vgl. Secunet (2001).

Rechnungslegung (IDW RS) und Prüfungshinweise (IDW PH) veröffentlicht werden[445], an denen sich die Branche bei ihrer Prüf- und Beratungstätigkeit rechtsverbindlich orientieren kann.

Von Bedeutung sind diese Standardisierungsbemühungen, da Abschlussprüfungen von Jahres- und Konzernabschlüssen durch Wirtschaftsprüfer integraler Bestandteil des Wirtschaftslebens sind und sich branchenübergreifend Wirtschaftsprüfer an diesen Normen orientieren. Die IDW Standards sind zwar nicht gesetzlich bindend, jedoch garantiert ihre Einhaltung dem Wirtschaftsprüfer Rechtsschutz, da diese Vorgaben durch Konsens in Politik und Rechtsprechung entwickelt werden. Weiterhin ist die begriffliche Klarstellung, die durch die IDW Publikationen vorangetrieben wird, für alle Marktteilnehmer von großem Interesse. IDW Veröffentlichungen haben nicht den Anspruch originäre Quellen zu generieren, sondern interpretieren vorhandene Gesetzestexte und wenden diese im Prüfungsalltag an.

Für den Einsatz von Informationstechnologie in allen Branchen, auch in der Banken- und Zahlungsverkehrslandschaft, sind die so genannten IDW RS FAIT 1 und FAIT 2 wegweisend.[446] In Zusammenhang mit den „Mindestanforderungen an die Interne Revision" der BAFin ist ferner IDW EPS 523 von Interesse, der speziell die Funktionsfähigkeit der Internen Revision von Kreditinstituten zum Gegenstand hat.[447] Er ist jedoch noch nicht endgültig verabschiedet und liegt lediglich als Entwurfsfassung vor (Stand Oktober 2003). Die Verknüpfung zum Risikomanagement und dessen Überprüfung stellt für Unternehmen, die teilweise im Besitz von Gebietskörperschaften sind, IDW PS 720 dar.[448]

5.1.1.4.1 Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie

Die Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie[449] (IDW RS FAIT 1) verdeutlichen die Notwendigkeit von Risikomanagementansätzen, in diesem Fall für die Bewältigung der entstehenden Risiken durch den Einsatz von IT zur Datenverarbeitung in Unternehmen im Allgemeinen und der Rechnungslegung im Besonderen. IDW RS FAIT 1 verlangt von allen Unternehmen – nicht nur Kreditinstituten – umfangreiche Maßnahmen zu den aus der klassischen Informatik bekannten Aspekten der Sicherheit von Informationen. Es müssen gewährleistet sein:

- Datensicherheit und Datenschutz,
- Vetraulichkeit, Integrität und Verfügbarkeit der Daten, sowie
- Autorisierung, Authentizität und Verbindlichkeit von Geschäftsvorfällen.

[445] Ein „E" vor den jeweiligen Kürzeln bedeutet, dass es sich bei dem jeweiligen Dokument um einen Entwurf in der Diskussion handelt, z. B. IDW EPS 523.
[446] RS steht für Stellungnahme zur Rechnungslegung. FAIT für Fachausschuss für Informationstechnologie im IDW.
[447] Vgl. IDW EPS 523 (2003).
[448] Vgl. 5.1.1.4.4.
[449] Vgl. IDW RS FAIT 1 (2002).

Abgebildet auf die Grundsätze ordnungsmäßiger Buchführung bei IT-gestützter Rechnungslegung bedeutet dies, dass folgende Kriterien, die sich im Handelsgesetzbuch wiederfinden, bei der Überprüfung des Unternehmens in Bezug auf die Buchführung und deren Datensätze erfüllt sein müssen:

- Vollständigkeit,
- Richtigkeit,
- Zeitgerechtheit,
- Ordnung,
- Nachvollziehbarkeit und
- Unveränderlichkeit.

Die Vorgaben von IDW RS FAIT 1 gehen bis zur Forderung, dass im Falle von Outsourcing-Maßnahmen das beauftragte Unternehmen die gleichen Kriterien wie das geprüfte Unternehmen erfüllen und nachweisen können muss. In weiterer Form finden sich über die Rechnungslegung hinausgehende Forderungen ähnlicher Art im IDW PS 330, der an dieser Stelle jedoch nicht vertiefend dargestellt wird.[450]

Es zeigen sich klar die Parallelen zu Risikomanagementsystemen, die in allgemeiner Art in Kapitel 5.2 und in spezifischer Art beim Management Operationeller Risiken in Kapitel 5.3 diskutiert werden.

5.1.1.4.2 Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce

Die Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce (IDW ERS FAIT 2) sind ebenso wie IDW RS FAIT 1 nicht ausschließlich für Finanzinstitute spezifiziert, sondern umfassen jegliche „Anbahnung und Abwicklung von Geschäftsvorfällen (von der Kontaktaufnahme bis zum Zahlungsverkehr) zwischen Marktteilnehmern in elektronischer Form.“[451]

Während in IDW RS FAIT 1 die grundlegenden Anforderungen an die Sicherheit von IT-Systemen in der Buchführung formuliert werden, beschäftigt sich IDW ERS FAIT 2 mit den besonderen IT-Risiken beim Einsatz von eCommerce-Systemen, sowohl bei der Kommunikation als auch bei der Verarbeitung von Transaktionsdaten. In einem ausführlichen Anhang werden den entsprechenden Risiken Anforderungen des IDW und mögliche Maßnahmen aus Unternehmenssicht gegenübergestellt.

Aufbauend auf IDW RS FAIT 1 werden die unternehmensbezogenen Vorgänge, die auf eCommerce-Aktivitäten zurückzuführen sind, betrachtet und mit Empfehlungen zum Umgang versehen. Im einzelnen sind dies:

- Belegfunktion,
- Journal- und Kontenfunktion,
- Dokumentation (der technischen Einrichtungen und Verfahren zur Datenbearbeitung),
- Aufbewahrungspflichten (nach HGB 10 Jahre für Daten mit Belegfunktion – auch und insbesondere bei angewandten Verschlüsselungsalgorithmen einzuhalten und nachzuweisen),
- spezielle Aufbewahrungspflichten beim Elektronischen Geschäftsverkehr,

[450] Vgl. IDW PS 330 (2002).
[451] IDW ERS FAIT 2 (2002), S. 879.

Abschließend wird in IDW ERS FAIT 2 das IT-Umfeld und die IT-Organisation bei Einrichtung und Einsatz von eCommerce-Systemen ausführlich diskutiert. Dies geschieht vorrangig in informierender Darstellung, weniger in paragraphenorientierter Abhandlung. Bezug wird demzufolge auch nicht auf Gesetzestexte genommen, sondern bei Detailfragen auf IDW RS FAIT 1.

5.1.1.4.3 Prüfung der Funktionsfähigkeit der Internen Revision bei Kreditinstituten: IDW EPS 523

Der IDW EPS 523[452] ergänzt branchenunspezifische Standards des IDW, die sich mit der Internen Revision beschäftigen, insbesondere IDW PS 260 „Das interne Kontrollsystem im Rahmen der Abschlussprüfung“[453] und IDW PS 321 „Interne Revision und Abschlussprüfung“[454], um bankspezifische Besonderheiten der Revision, die rechtlich verbindlich in den Anforderungen der BAFin ihren Niederschlag finden.

In IDW EPS 523 werden ausführlich die organisatorischen Voraussetzungen der Funktionsfähigkeit der Internen Revision dargelegt, beginnend mit einer schriftlich fixierten Ordnung des gesamten Geschäftsbetriebs bis hin zur mit Kontrollen unterlegten Ablauforganisation des Unternehmens. Die hervorgehobene Stellung der Internen Revision im Unternehmen, ihre Befugnisse und das uneingeschränkte Informationsrecht sowohl intern als auch gegenüber ausgelagerten Geschäftsbereichen und -tätigkeiten wird betont. Die zur Aufgabenerfüllung notwendigen Sach- und Personalressourcen sind zwingende Voraussetzung für die erfolgreiche Abschlussprüfung eines Unternehmens. Die Anforderungen an den Revisionsprozess im Hinblick auf eine risikoorientierte Prüfungsplanung und -durchführung nehmen im IDW EPS 523 ebenso wie die Berichterstattung und Qualitätssicherung einen breiten Raum ein. Der vom Wirtschaftsprüfer anzufertigende Prüfbericht über die Arbeit der Internen Revision muss im Wesentlichen die vorgenannten Punkte und die darin gestellten Anforderungen abhandeln. Der Bezug zu aufsichtlichen Vorgaben an die Interne Revision (MaIR, siehe Abschnitt 5.1.1.2.3) muss im Abschlussbericht des Wirtschaftsprüfers explizit hergestellt und die Einhaltung dieser Vorgaben beurteilt werden.

5.1.1.4.4 IDW Prüfungsstandard 720 gemäß § 53 HGrG

Für die Jahresprüfung oder die Prüfberichte einer Gesellschaft, die mindestens mit Sperrminorität der öffentlichen Hand gehört, kann die Gebietskörperschaft nach § 53 HGrG[455] eine Prüfung der Gesellschaft durch Wirtschaftsprüfer beantragen. Dieser wendet IDW Prüfungsstandard 720: „Fragenkatalog zur Prüfung der Ordnungsmäßigkeit der Geschäftsführung und der wirtschaftlichen Verhältnisse“ nach § 53 HGrG an, und prüft neben dem eingesetzten Risikomanagementsystem die Datenverarbeitung und deren Übereinstimmung mit gesetzlichen Vorschriften und anerkannten Regeln.[456] Die untersuchten Teilgebiete nach IDW PS 720 umfassen im Einzelnen die Gebiete:

- Datenverarbeitungs(DV)-Umfeld und DV-Organisation
- Softwareentwicklung/-pflege
- DV-Produktion
- Netzwerk

[452] Vgl. IDW EPS 523 (2003).
[453] Vgl. IDW PS 260 (2001).
[454] Vgl. IDW PS 321 W(2002).
[455] Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder (Haushaltsgrundsätzegesetz).
[456] Vgl. IDW PS 720.

- Zugriffssicherung/Benutzerberechtigungen
- Datensicherung/Wiederanlauf
- Ausfallsicherung
- Physische Sicherung
- Vertragliche Regelungen
- Dokumentation der Hardwareumgebung
- Dokumentation der Software

5.1.1.5 Anforderungen aus dem Zentralen Kreditausschuss

In den Arbeitsstäben, den Arbeits- und Projektgruppen des ZKA werden technische Spezifikationen erarbeitet, oder bei Dienstleistern in Auftrag gegeben. Bei diesen Spezifikationen handelt es sich in erster Linie um technische Ausführungen, sicherheitsrelevante Fragestellungen werden auf Komponentenebene bearbeitet. Management von Sicherheit aus Organisationssicht oder in einem ganzheitlichen Ansatz spielt nur in allgemeinen Formulierungen vom Stil „besondere Umsicht" oder „hat Sicherheit zu garantieren" eine Rolle.
In Münch (2002) werden drei Themengebiete unterschieden, in denen der ZKA Anforderungen im Bereich Zahlungsverkehr entwickelt: 1) technische Systeme mit Kundenkontakt (Geldautomaten, Kartenterminals etc.), 2) Homebankingsysteme und 3) Zahlungsverkehrssysteme.[457] Technische Spezifikationen betreffen insbesondere alle Kommunikationsgeräte und -kanäle, die von außerhalb der Bank in diese hinein führen. Beispiele für technisch orientierte ZKA-Spezifikationen aus den Themengebieten 1 und 2 sind der HBCI-Standard, die Vorgabe von Klasse-3-Kartenlesern für die Geldkarte, die SmartCard-Spezifikationen, Vorgaben für ATMs, für POS-Geräte aber auch Vorgaben für externe Netzbetreiber, beispielsweise Telecash, wie deren Terminals und Datenformate auszusehen haben, und welche sonstigen Bedingungen ein Netzbetreiber, beispielsweise im Hinblick auf Verschlüsselungsalgorithmen, erfüllen muss. Während bei den Komponenten die Vorgaben sehr detailliert sind und der ZKA auch als Zulassungsinstanz für neue Geräte im Markt agiert, fühlt sich der ZKA im Bereich IT-Sicherheit im Zahlungsverkehr nur am Rande zuständig:[458] „Zu Fragen der Sicherheit von im Zahlungsverkehr eingesetzten IT-Systemen nimmt man die Position ein, dass die Sicherheit von den Betreibern der Systeme zugesichert und daher auch umzusezten ist. Deshalb geht man hier davon aus, dass die technischen Systeme sicher sind."

Die Organisation der Bank selber unterliegt keinen ZKA-Normen, höchstens werden Vorgaben zum Routing von Daten durch Bankennetzwerke gemacht.

Im nicht-technischen Bereich liegt der Fokus des ZKA nicht auf sicherheitsrelevanten Fragestellungen. Vielmehr liegt die Bedeutung des ZKA darin, Standards für bankübergreifende Geschäftsprozesse gemeinsam zu erarbeiten und diese zu pflegen. Zwar werden im ZKA lediglich Selbstverpflichtungen der Branche vereinbart, die jedoch im Bereich der Standardisierungsvorgaben im Hinblick auf die effiziente Abwicklung im Massengeschäft von großer Bedeutung sind. Sanktionierung von Instituten, die intern andere Vorgaben beschließen, sind weder möglich noch notwendig, da die übergreifende Zusammenarbeit, beispielsweise beim Datenaustausch, einheitliche Standards (u.a. EDIFACT) erforderlich macht. Auf der Ebene der nicht-technischen Geschäftsprozesse sind beispielhaft die in Zusammenarbeit mit der Deutschen Bundesbank erarbeiteten Zahlungsverkehrsabkommen (allerdings mit Vertragscharakter) zu nennen, die Prozedere und Haftungsverpflichtungen bei Überweisungen, Scheckeinreichungen und Lastschriften regeln. Ohne derartige Abkommen

[457] Vgl. Münch (2002), S. 35 ff.
[458] Münch (2002), S. 37

wäre eine Verflechtung der deutschen Banken- und Sparkassenlandschaft im Gironetz, wie sie in Abbildung 8 zum Ausdruck kommt, nicht oder nur zu ungleich höheren Kosten realisierbar.

Die Problematik komplexer Zusammenhänge und schneller technologischer Entwicklungen versucht der ZKA durch ein zweigeteiltes Prozedere bei Vereinbarungen zu umgehen. In den Beschlussgremien werden Vereinbarungstexte verabschiedet, die grobe Leitlinien und allgemeine Formulierungen enthalten. Die Detailfragen werden in den Fachausschüssen geklärt und dort als Anhang zu den Vereinbarungen festgehalten. Ändern sich technische Details können diese Anhänge von den Fachausschüssen modifiziert werden, ohne dass die Rahmenvereinbarung neu verhandelt werden muss.

Auf europäischer Ebene zeigen sich die Schwierigkeiten branchenweiter Standardisierungsarbeit auf dem Weg zur Single European Payment Area deutlich. Eine kostengünstige europäische Überweisung wurde erst durch die EU-Richtlinie über grenzüberschreitende Überweisungen (97/5/EG) erzwungen, die europäische Lastschrift steht zwar auf der Agenda der europäischen Bankenwelt, ist jedoch noch nicht realisiert. Ein Grund für die Probleme auf europäischer Ebene sind die noch fehlenden oder gerade erst im Aufbau befindlichen Institutionen, die sich wie der ZKA Standardisierungsfragen widmen und über entsprechende Befugnisse verfügen.

5.1.1.6 Bundesamt für Sicherheit in der Informationstechnik: Anforderungen an Banken

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet keine detaillierten Vorgaben für die Sicherheit elektronischer Bezahlsysteme im Besonderen oder Banken im Allgemeinen. Als Bundesbehörde wird das Amt auf Anfrage durch andere Bundesbehörden oder Eigeninitiative tätig, kann Studien vergeben, beispielsweise im Rahmen der Analyse kritischer Infrastrukturen eine Untersuchung der IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, und daraus folgend Empfehlungen abgeben.[459] Spezifische Fragestellungen kann das BSI gemeinsam mit den relevanten Akteuren auf Anfrage bearbeiten. Beispielsweise werden bei der Bewertung der Sicherheit des Electronic Banking mit den Kreditunternehmen gemeinsam Vorgaben erarbeitet – wiederum in Einklang mit Vorgaben auf EU- und internationaler Ebene. Grundlegende Arbeiten, auf die das BSI referenziert, finden sich im Zusammenhang mit Electronic Banking bei der Bank für Internationalen Zahlungsausgleich, die 2003 sowohl Vorgaben für nationale wie für grenzüberschreitende Anwendungen herausgegeben hat.[460]

Die bislang wesentliche Tätigkeit des BSI in Bezug auf unternehmensübergreifende sicherheitsrelevante Fragestellungen ist die beständige Aktualisierung des Grundschutzhandbuchs.[461]

5.1.2 Vorgaben auf europäischer Ebene

5.1.2.1 Europäische Union

„Der bestehende Rechtsrahmen für den Zahlungsverkehr stützt sich weitgehend auf nationale Rechtsvorschriften.“[462] Zu diesem Schluss kommt die Europäische Kommission im Dezember 2003 in ihrer Mitteilung an den Rat und das Europäische Parlament in einem Konsultations-

[459] Vgl. Münch (2002).
[460] Vgl. BIZ (2003j) und BIZ (2003i).
[461] Vgl. BSI (2000). Aktuellster Stand der vom BSI vertriebenen CD-Rom ist Mai 2003. Vgl. ausführlicher 5.2.3.1.
[462] KOM (2003b), S. 2.

papier, in dem „Ein neuer Rechtsrahmen für den Zahlungsverkehr im Binnenmarkt“ diskutiert wird. Für den Aspekt (technischer) Sicherheit im Zahlungsverkehr, den die Europäische Union sich allerdings auch nie auf die Agenda geschrieben hat, mag diese Aussage stimmen. Der nationale Zahlungsverkehrsrahmen ist in Teilen gerade in den letzten Jahren erheblich von EU-Recht geprägt worden (siehe Abbildung 21). Insbesondere die Verordnung 2560/2001/EG hat mit ihrer klaren Preisvorgabe – Überweisungen unter 12.500 Euro dürfen in Euroland nicht mehr kosten als im Inland – eine veränderte Zahlungsverkehrslandschaft in Europa angestoßen, da ihre Umsetzung ohne Kooperationen im Finanzsektor auf europäischer Ebene nicht denkbar gewesen wäre.

Die Sicherheit elektronischer Zahlungsverfahren insbesondere im Hinblick auf Konsumentenschutz genießt bei der Europäischen Kommission höchste Priorität.[463] Dies verdeutlichen die verschiedenen Empfehlungen der EU zum elektronischen Zahlungsverkehr und die eingeleiteten Maßnahmen zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln. Gleichwohl beziehen sich diese Maßnahmen nicht auf einzelne Vorgaben zur sicheren Gestaltung des Zahlungsverkehrs, dafür ist der europäische Markt für Zahlungssysteme im Retail-Bereich viel zu unübersichtlich. Vielmehr geht es um eine weitere Harmonisierung der nationalen Rechtssysteme, beispielsweise müssen einheitliche Straftatbestände definiert werden, die EU-weit als solche gelten.[464]

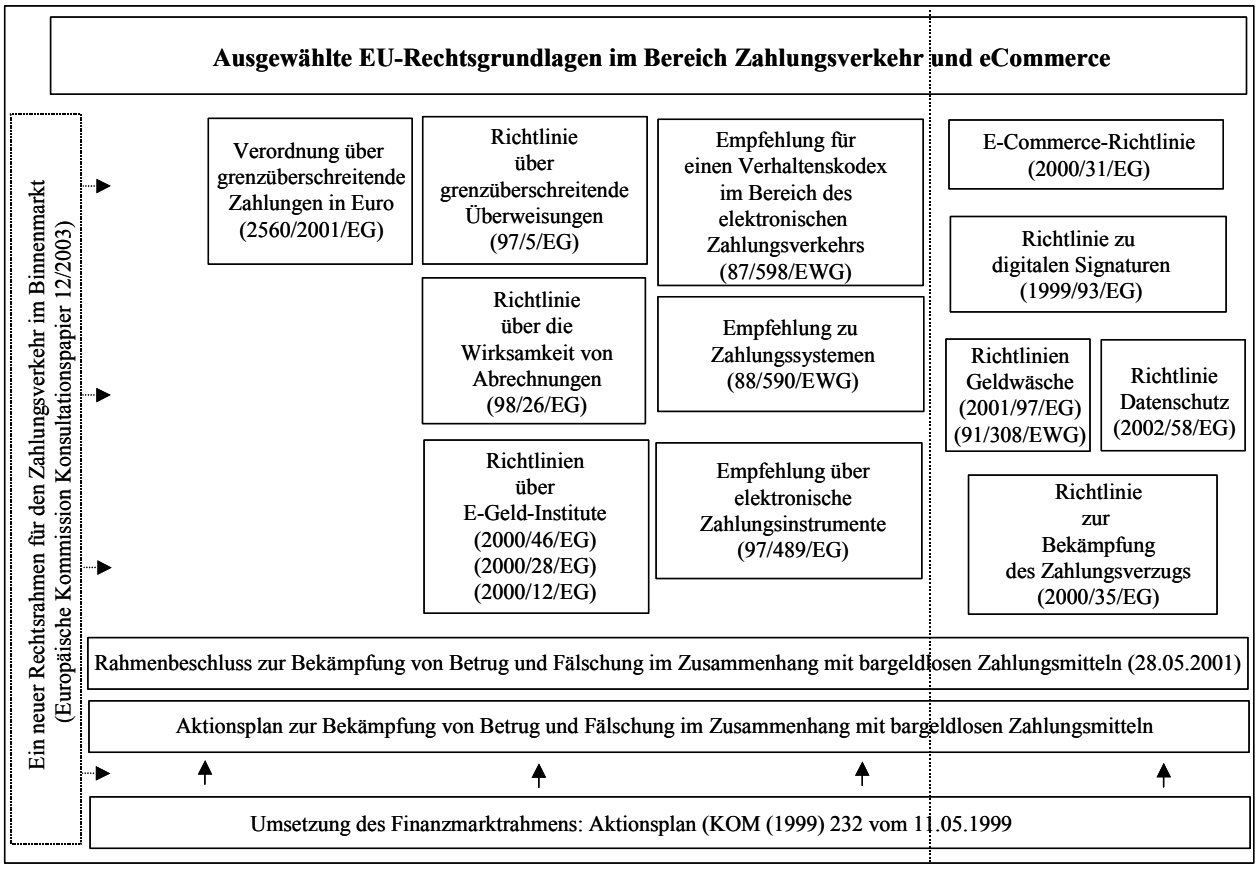

Abbildung 21: Ausgewählte Rechtsvorschriften der EU für den (Massen-)zahlungsverkehr

[463] Die Kommission kann sich dabei auf den Auftrag aus Artikel 153 EG-Vertrag beziehen, der dem Verbraucherschutz höchste Priorität einräumt. Dabei legt die Kommission den Begriff ‚Verbraucher’ weit aus: Konsument, Einzelhändler, KMU und andere Zahlungsdienstleistungsnutzer. (KOM (2003b), S.15 FN 21).
[464] Vgl. EU (2001).

Die verschiedenen Richtlinien und Empfehlungen im Bereich Zahlungsverkehr, die in Abbildung 21 aufgeführt sind, betonen mehr oder minder deutlich die Notwendigkeit sicherer Zahlungssysteme auf juristischer Ebene. Es gilt den Konsumenten ebenso vor kriminellen Handlungen zu schützen wie den Händler, der beispielsweise seine Waren über das Internet vertreibt. Die zunehmende Ausgestaltung des Rechtsraums im Internet, namentlich im eCommerce, bleibt auch für die Sicherheit der Zahlungssysteme auf mittlere Sicht nicht ohne Folgen. Beispielsweise wird die rechtsgültige digitale Signatur, ihren Erfolg bei den Anwendern vorausgesetzt, einige der herkömmlichen Authentifizierungsprobleme im Zahlungsverkehr lösen können – natürlich nicht, ohne neue Probleme in anderen Segmenten zu generieren.[465]

Der Zahlungsverkehr ist für die EU nur im Bereich Massenzahlungsverkehr relevant. Der Großzahlungsverkehr wird von den Zentralbanken und Aufsichtsbehörden hinlänglich überwacht, zudem sind in diesem Segment kaum Endkonsumenteninteressen berührt. Mit dem von der Kommission vorgelegten Konsultationspapier, das „Einen neuen Rechtsrahmen für den Zahlungsverkehr im Binnenmarkt“ vorschlägt und diskutieren möchte, greift die Europäische Kommission viele Probleme im grenzüberschreitenden Zahlungsverkehr explizit auf, stellt ihre eigene Position umfassend zur Diskussion und strebt zumindest von der legislativen Seite eine Lösung an.

Im Hinblick auf die Sicherheit des Zahlungsverkehrs nimmt die Kommission in ihrem Konsultationspapier eine klare Position ein: „Nach Auffassung der Kommission gebührt den Bemühungen, die Sicherheit im Zahlungsverkehr zu steigern und zur Bekämpfung von Zahlungsbetrug [...] beizutragen, hohe Priorität. Obwohl es in erster Linie Sache des Zahlungsverkehrssektors ist, für die unter Wirtschaftlichkeitsgesichtspunkten bestmögliche Sicherheitsinfrastruktur für die Zahlungsdienste zu sorgen, sollte die Frage der rechtlichen Sicherung des Zahlungsumfelds im Neuen Rechtsrahmen geregelt werden.“[466] Erklärtes Ziel dieser Regelungen ist die technische Neutralität des Rechtsrahmens.[467]

In einem ausführlichen Anhang werden im Konsultationspapier zum neuen Rechtsrahmen zahlreiche offene Probleme im grenzüberschreitenden Zahlungsverkehr adressiert und Vorschläge zu deren Lösung unterbreitet. In Bezug auf die Sicherheit der Zahlungssysteme im weiteren Sinne sind folgende Themengebiete von Relevanz:[468]

- Bewertung der Sicherheit von Zahlungsinstrumenten und -komponenten: hier geht es vor allem um geeignete Verfahren die Sicherheit von Zahlverfahren zertifizierbar zu gestalten und die Ergebnisse der Zertifizierung EU-weit zu akzeptieren.
- Alternative Streitbeilegung: Es sollen für alle grenzüberschreitenden Zahlverfahren außergerichtliche Streitbeilegungsprozeduren geschaffen werden, um das Vertrauen der Anwender zu stärken.
- Widerrufbarkeit von Zahlungsaufträgen: Bislang fehlen auf europäischer Ebene klare Regeln zu Widerrufsrechten, wie sie etwa bei der Lastschrift in Deutschland existieren.

[465] Ein typisches Problem digitaler Signaturen betrifft die Haftung für verlorengegangene/ entwendete Signaturen. Hiermit kann in weit größerem Umfang Missbrauch betrieben werden als mit einer entwendeten PIN, die nur einen begrenzten Einsatzbereich hat. Eine ähnliche Thematik wurde allerdings bereits mit dem Aufkommen der Unterschrift via Fax diskutiert.
[466] KOM (2003b), S. 13f.
[467] Vgl. KOM (2003b), S. 17.
[468] Vgl KOM (2003b), S. 24ff.

- Rolle des Zahlungsdienstleistungsanbieters im Falle von Streitigkeiten zwischen Kunden und Händlern beim Fernabsatz: Der EU-weite Handel wird durch fehlende juristische Regelungen im Streitfall behindert. Der Konsument hat zwar teilweise weitreichende Rechte, die Möglichkeiten, diese auch in anderen Ländern wahrzunehmen sind bislang eingeschränkt.
- Nicht erfolgte oder mangelhafte Abwicklung einer Zahlung: Bislang fehlen eindeutige Haftungsregeln, die bei fehlerhafter Abwicklung für Konsumenten und Händler greifen.
- Pflichten und Haftung der Vertragsparteien bei nicht genehmigten Transaktionen: Es gilt für alle Zahlarten, nicht nur für Kartenzahlungen, eine belastbare Grundlage zu schaffen, auf die im Falle der betrügerischen Verwendung von Zahlungssystemen Streitigkeiten ausgetragen werden können.
- Sicherheit der Netze: Es gilt der zunehmenden Cyberkriminalität einerseits mit deutlichen Signalen in Bezug auf die Strafverfolgung zu begegnen, andererseits die Sicherheit der Netze überprüfbar zu gewährleisten.
- Störungen im Zahlungsnetz und daraus resultierende Haftungsfragen sind bislang im EU-Recht nicht einheitlich geklärt.

5.1.2.2 Europäische Zentralbank

Die EU geht davon aus, dass sicherheitstechnische Fragestellungen im Hinblick auf Zahlungssysteme im Groß- und Massenzahlungsverkehr in die Befugnis der EZB fallen.[469] Die Befugnisse sind de jure in der ESZB-Satzung angelegt. Die EZB kann neben Empfehlungen und Stellungnahmen nach Artikel 12 Absatz 1 und Artikel 14 Absatz 3 ESZB-Satzung Leitlinien erlassen und ebenso Verordnungen, die über nationalem Recht stehen.

Im Bereich Großzahlungen ist die EZB bereits mit ihrer Leitlinienkompetenz in Erscheinung getreten und hat als (Teil-)Betreiberin des Systems TARGET die EZB Leitlinie EZB/2001/3 über ein trans-europäisches automatisiertes Echtzeit-Brutto-Express-Zahlungsverkehrssystem veröffentlicht und mit der TARGET-Leitlinie EZB/2002/1 aktualisiert. In diesen Leitlinien werden der Betrieb, der Zugang und die Sicherungs- und Notfallmaßnahmen des Zahlungssystems TARGET einschließlich der daran angeschlossenen RTGS-Systeme geklärt und über Anhänge zusätzliche Details geregelt.[470] Leitlinien der EZB gelten ausschließlich für Teilnehmer am Eurosystem, mit den übrigen europäischen Ländern wurden analoge separate Vereinbarungen getroffen, um einen Zugang zu TARGET zu erhalten.[471]

Weitere Rechtsinstrumente sind von der EZB bislang weder zu Massen- noch zu Großbetragszahlungssystemen verabschiedet worden. Gleichwohl sieht sich die EZB in ihrer Funktion als Aufseher über den Zahlungsverkehr im Euroraum jederzeit in der Lage einzugreifen, wenn Entwicklungen nicht in die gewünschte Richtung verlaufen. Überwachungsstandards können von der EZB wie im Falle der „Core Principles for Systemically Important Payment Systems" für eigene Zwecke übernommen werden, in diesem Fall für die Anforderungen an die Sicherheit von Großbetragszahlungssystemen. Sie können aber auch vom ESZB selbst entwickelt werden, sofern die EZB zur Überzeugung gelangt marktrelevante Entwicklungen würden angemessene Standards erfordern. Die Entwicklung innovativer Zahlungsprodukte im gesamten Euroraum wird deshalb von der EZB mit Interesse verfolgt.[472]

[469] KOM (2003b), S. 20.
[470] Vgl. EZB (2001), EZB (2002).
[471] EZB (2002b), S. 54.
[472] EZB (2000), S. 3, EZB (2002b), S. 57.

Für den Bereich des Massenzahlungsverkehrs wurde ein Anforderungskatalog erstellt, der eng an die Core Principles for Systemically Important Payment Systems (CPSIPS) angelehnt ist.[473] Dieser Katalog dient als Grundlage der Überprüfung der in Europa aktiven Massenzahlungssysteme. Es werden drei Kategorien von Systemen unterschieden: Systemrelevante Massenzahlungssysteme, solche von besonderer Bedeutung und die übrigen. Es obliegt den nationalen Zentralbanken, die regelmäßige Überprüfung der nationalen Massenzahlungssysteme vorzunehmen. Gegenwärtig läuft die Kategorisierung aller im Gebiet des ESZB eingesetzten Verfahren. Diese soll bis Ende 2004 abgeschlossen sein.

Ein systemrelevantes Massenzahlungssystem ist durch folgende Faktoren charakterisiert:[474]

- Marktdurchdringung: Das System besitzt einen Marktanteil von mehr als 75 % am Gesamtmarkt für Massenzahlungen.
- Finanzielle Risiken: Ein System erzielt mehr als 10 % der vom nationalen RTGS-System verarbeiteten Werte oder erreicht einen tagesdurchschnittlichen Umsatz von mehr als 10 Mrd. Euro.
- Dominoeffekt: Die Gefahr, dass der Ausfall eines Teilnehmers die anderen negativ beeinflusst ist besonders hoch, wenn die Netting-Rate 10 % oder weniger beträgt, oder die Netto-Sollposition der Teilnehmer mindestens 1 Mrd. Euro erreicht. Ebenso gilt ein Konzentrationsgrad von 80 % als kritisch.[475]

Grundsätzlich müssen nach der Vorstellung der EZB die Betreiber systemrelevanter Massenzahlungssysteme alle CPSIPS erfüllen.

Für die Massenzahlungssysteme von besonderer Bedeutung wird als Mindestanforderung die Einhaltung der Grundprinzipien I (rechtliche Grundlagen), II (Einschätzung finanzieller Risiken), VII (Sicherheit und Zuverlässigkeit), VIII (effiziente Abwicklung), IX (Zugangskriterien) und X (transparente Führungsstruktur) erwartet. Ein System von besonderer Bedeutung ist gekennzeichnet durch einen Marktanteil von mehr als 25 %. Dabei werden nur Systeme, die nach dem Prinzip des Automated Clearing Houses (ACH) organisatorisch aufgebaut sind, oder aber multilaterale Vereinbarungen mit Vertragscharakter beinhalten, berücksichtigt. Bilaterale Vereinbarungen und deren Bündelung sind von den Betrachtungen der EZB ausgenommen.

Für die übrigen Systeme gilt, dass sie die jeweiligen nationalen Standards, sofern vorhanden, erfüllen müssen aber keinen spezifischen Anforderungen des ESZB unterworfen sind.

Ziel ist es aus Sicht der EZB, mit diesen Standards ihrem Auftrag entsprechend „das reibungslose Funktionieren von Massenzahlungssystemen, die für die Wirtschaft von großer Bedeutung sind, sowie Effizienz, Sicherheit und Wettbewerbsgleichheit für die Teilnehmer verschiedener Systeme zu gewährleisten und um letztendlich das Vertrauen der Öffentlichkeit in den Euro zu stärken.“[476] Während für die Individual-Zahlungssysteme von der BIZ neben den Grundprinzipien auch ein erläuternder Zusatztext erarbeitet wurde, der als Hilfestellung der recht abstrakt gehaltenen CPSIPS dient, ist aufgrund der Kürze der Zeit ein solcher

[473] Vgl. EZB (2003d). Zu den CPSIPS vgl. im Detail 5.1.3.1.2.
[474] Vgl. EZB (2003d), S. 2ff. Zusätzlich können nationale Zentralbanken Sonderfaktoren berücksichtigen und auch bei Nichterfüllung der drei Faktoren ein System als systemrelevant werten.
[475] Netting-Rate: Netto-Verrechnungssaldo in Prozent des Brutto-Transaktionswerts (EZB (2003d), S. 3 FN 6). Ein Konzentrationsgrad von 80 % ist erreicht, wenn die 5 größten Teilnehmer am System 80 % des Brutto-Umsatzes generieren.
[476] EZB (2003a), S. 77.

Leitfaden für den Massenzahlungsverkehr noch nicht entstanden. Daher bleibt es unter dem Aspekt der Sicherheit bei relativ vagen aber anspruchsvollen Formulierungen der Art „Die Massenzahlungssysteme von besonderer Bedeutung sollten daher sicher sein und sich durch einen zuverlässigen Betrieb sowie durch geeignete Notfallverfahren auszeichnen." oder „Allerdings müssen Sicherheit und Effizienz in einem ausgewogenen Verhältnis zueinander stehen. [...] Systembetreiber sollten daher abwägen, welche Instrumente des Risikomanagements für ihr System am besten geeignet sind."[477]

Ein weiteres Feld innovativer Entwicklung stellt eGeld dar. Die EZB hatte bereits 1998 im „Bericht über elektronisches Geld" angemessene technische, organisatorische und verfahrensmäßige Sicherungen für eGeld-Systeme gefordert. In den letzten zwei Jahren wurden in der Folge der Weiterentwicklung von eGeld-Systemen in der EU Sicherheitsziele im Zahlungsverkehr mit elektronischem Geld entwickelt.[478] Die „Electronic Money System Security Objectives" (EMSSO) sind an der Methodologie der Common Criteria (ISO/IEC 15408) orientiert und wurden nach einer öffentlichen Konsultationsphase im Mai 2003 veröffentlicht.[479] Interessant ist diese Vorgabe unter anderem, da sie auf formalen Sicherheitskonzepten basiert, und in der Weiterentwicklung dieses Ansatzes unter Umständen technische Details behandelt werden, die sich bislang in den offiziellen Sicherheitsvorgaben der Regulatoren in dieser Form nicht finden. Angedacht ist die Weiterentwicklung der EMSSO hin zu in den Common Criteria so genannten Schutzprofilen (Protection Profiles).[480] Die EMSSO stellen aus Sicht der EZB mit der dort durchgeführten Risikoanalyse, den identifizierten Bedrohungen/Risiken und den daraus abgeleiteten Schutzzielen die Basis der Bewertung der Sicherheit von E-Geld-Systemen dar, die innerhalb des ESZB eingesetzt werden.[481] Die Überprüfung der Sicherheit solcher Systeme obliegt ausschließlich den nationalen Zentralbanken.

5.1.3 Internationale Vorgaben

5.1.3.1 Vorgaben der Bank für Internationalen Zahlungsausgleich

5.1.3.1.1 Lamfalussy-Standards

Der Rahmen für das Risikomanagement von multilateralen Netto-Großzahlungssystemen wurde bereits 1990 im sogenannten Lamfalussy-Report vorgegeben.[482] In diesem werden die sechs Lamfalussy-Kriterien aufgestellt, die zur Beurteilung von Nettosystemen herangezogen werden (siehe Tabelle 5). Nettosysteme waren zu diesem Zeitpunkt, nicht zuletzt aufgrund technischer Restriktionen bei der Echtzeitverarbeitung, die führenden Verfahren im Großzahlungsverkehr. Systeme, die den gleichzeitigen Ausfall mehrer Teilnehmer (eine aus Sicht des systemischen Risikos besonders gefährliche Situation) verkraften, heißen Lamfalussy plus-compliant oder Lamfalussy plus-Systeme.

Die „Core Principles for Systemically Important Payment Systems" sind eine Weiterentwicklung der Anforderungen an heute eingesetzte Zahlungssysteme.

[477] EZB (2003d), S. 6 und S. 8.
[478] Vgl. EZB (1998b).
[479] Vgl. EZB (2002a), EZB (2003b).
[480] Vgl. EZB (2003b), S. 5.
[481] Vgl. EZB (2003b), S. 5.
[482] Vgl. BIZ (1990).

I	Netting-Verfahren benötigen eine wohlbegründete Rechtsgrundlage
II	Die finanziellen Risiken beim Netting müssen den Teilnehmern bewusst sein
III	Multilaterale Netting-Systeme brauchen festgelegte Verfahren für das Management von Bonitäts- und Liquiditätsrisiken mit klaren Zuständigkeiten
IV	Auch wenn der Teilnehmer mit der größten einzelnen Nettoschuldnerposition seine Ausgleichszahlung nicht leisten kann, muss das System in der Lage sein, den täglichen Saldenausgleich herzustellen
V	Objektive und öffentlich bekanntgegebene Zulassungskriterien für Netting-Systeme sind Voraussetzung
VI	Die Netting-Systembetreiber müssen die Zuverlässigkeit der technischen Einrichtungen sicherstellen und Ausweicheinrichtungen bereitstellen

Tabelle 5: Die Lamfalussy-Kriterien[483]

5.1.3.1.2 Core Principles for Systemically Important Payment Systems

Aufbauend auf dem Lamfalussy-Report erfolgte beim Committee on Payment and Settlement Systems (CPSS) die Weiterentwicklung von allgemeingültigen Kriterien für sichere Zahlungssysteme.[484] Während die Lamfalussy-Kriterien stark von der Betrachtung von Netting-Systemen geprägt waren, aber bereits in den neunziger Jahren auch auf andere Zahlungssysteme oder Clearing- und Settlementverfahren angewendet wurden, wurde mit den Core Principles for Systemically Important Payment Systems (CPSIPS) versucht, allen systemisch wichtigen Verfahren gerecht zu werden – unabhängig vom zugrundeliegenden Ablauf (Kredit-/Debitmechanismen, elektronisch/manuelle Verarbeitung, elektronisch/beleggebundene Verarbeitung).[485] Dazu wurden die sechs Lamfalussy-Kriterien im Wesentlichen modernisiert und vier weitere Grundsätze aufgenommen (siehe Tabelle 6).[486]

Die Prinzipien sind mit Absicht allgemein gehalten, der erste Teil des BIZ-Reports beinhaltet lediglich 14 Seiten. Ziel ist es, mit den Prinzipien von technologischen Entwicklungen weitgehend unabhängig und „zeitlos“ zu bleiben. Gleichwohl bietet die BIZ in Teil 2 der Ausführungen auf weiteren 50 Seiten detaillierte Empfehlungen zur Umsetzung der Grundprinzipien.

Die Core Principles berücksichtigen den erweiterten Sicherheitsbegriff (siehe Abbildung 4: Der erweiterte Sicherheitsbegriff im Zahlungsverkehr) nahezu vollständig. Insbesondere werden die rechtlichen Rahmenbedingungen, unter denen Zahlungssysteme betrieben werden, explizit adressiert (Prinzip I). Ebenso soll das systemische Risiko, das gesellschaftliche Auswirkungen haben könnte, minimiert werden (Prinzipien IV, V und VI). Organisatorische Belange werden in Prinzip III widergespiegelt; es wird erwartet, das systemimmanente Anreize zur Beherrschung und Begrenzung der Risiken vorhanden sind.

[483] BIZ (1990).
[484] Vgl. BIZ (2001b eng.).
[485] Vgl. BIZ (2001b), S. 2.
[486] Vgl. BIZ (2000a), S. 14.

I	Das System sollte in allen betroffenen Rechtsordnungen eine solide Rechtsgrundlage aufweisen.
II	Die Regelungen und Verfahren des Systems sollten den Teilnehmern eine klare Einschätzung der Auswirkungen des Systems auf alle finanziellen Risiken, die sie mit ihrer Teilnahme eingehen, ermöglichen.
III	Das System sollte über klar definierte Verfahren für das Management von Kredit- und Liquiditätsrisiken verfügen, die auch die jeweiligen Verantwortungsbereiche der Systembetreiber und der Teilnehmer festlegen, und die angemessene Anreize für die Beherrschung und Begrenzung dieser Risiken enthalten.
IV	Das System sollte einen frühzeitigen endgültigen Ausgleich am Valutatag anbieten, vorzugsweise während des Tages, mindestens jedoch am Ende des Tages.
V	Ein System mit multilateralem Netting sollte zumindest in der Lage sein, den rechtzeitigen Abschluss des täglichen Saldenausgleichs auch dann sicherzustellen, wenn der Teilnehmer mit der grössten einzelnen Abrechnungsverbindlichkeit seine Ausgleichszahlung nicht leisten kann.
VI	Die für den Saldenausgleich verwendeten Aktiva sollten vorzugsweise eine Forderung an die Zentralbank sein; werden andere Aktiva verwendet, sollten sie mit geringen oder keinen Kredit- und Liquiditätsrisiken verbunden sein.
VII	Das System sollte in hohem Maße Sicherheit und Zuverlässigkeit des Betriebs sicherstellen und über Notfallverfahren für den rechtzeitigen Abschluss der täglichen Verarbeitung verfügen.
VIII	Das System sollte einen praktischen und ökonomisch effizienten Weg für Zahlungen bieten.
IX	Das System sollte über objektive und öffentlich bekanntgegebene Teilnahmekriterien verfügen, die einen gerechten und offenen Zugang ermöglichen.
X	Die Führungs- und Verwaltungsstruktur des Systems sollte effizient, rechenschaftspflichtig und transparent sein.

Tabelle 6: Core Principles for Systemically Important Payment Systems[487]

Von Bedeutung für die (IT-)Sicherheit von Zahlungssystemen in offenen Netzen ist das Grundprinzip VII „Das System sollte in hohem Maße Sicherheit und Zuverlässigkeit des Betriebs sicherstellen und über Notfallverfahren für den rechtzeitigen Abschluss der täglichen Verarbeitung verfügen." Die BIZ betont ausdrücklich, dass aufgrund des hohen Komplexitätsgrades der bei den Zahlungssystemen eingesetzten Technologien bei gleichzeitigem schnellem Wandel der verwendeten Techniken keine eindeutigen technischen Spezifikationen festgelegt werden können. Vielmehr werden in den Umsetzungshinweisen Risikomanagementaspekte betont.[488] Es wird von den Zahlungssystembetreibern erwartet, dass sie angemessene Maßnahmen ergreifen, um sowohl die Sicherheit der eigenen Komponenten des

[487] BIZ (2001b), S. 4.
[488] Vgl. BIZ (2001b).

Systems als auch das Zusammenspiel der Komponenten mit Marktteilnehmern, die an das System angeschlossen sind, zu gewährleisten. Dieser ganzheitliche Ansatz sollte durch die Einhaltung internationaler Standards (und deren Überprüfung durch interne und externe Revisoren) wie beispielsweise zur Informationstechnologie und -sicherheit (ISO/IEC TR13335, BSI 7799:1999 (mittlerweile ISO/IEC 17799)) aber auch zur Qualitätssicherung (ISO 9000 ff.) verfolgt werden. Als Grundlage der Bemühungen der Betreiber um eine möglichst hohe Sicherheit der Systeme werden klar formulierte und kommunizierte Sicherheitsziele und Sicherheitsgrundsätze gesehen, die insbesondere die Aspekte Vertraulichkeit, Integrität, Authentifizierung, Nichtbestreitbarkeit, Verfügbarkeit und Überprüfbarkeit umfassen. Die Ausführungen der BIZ zu diesen Punkten und zu den geforderten Analysen des Sicherheitsrisikos sind stark an die einschlägigen Publikationen zum Risikomanagementprozess angelehnt.[489]

Die CPSIPS behandeln unter den Ausführungen zu Grundprinzip VII unter den Punkten Sicherheit, Zuverlässigkeit und Aufrechterhaltung des Systembetriebs für den Bereich Zahlungssysteme die gleichen Themen, die auch beim "Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" adressiert werden (u. a. Infrastruktur, Personalqualifikation, Redundanzen). Allerdings gehen die Forderungen des White Paper in Einzelpunkten deutlich über die der CPSIPS hinaus. Beispielsweise werden in den CPSIPS redundante Systeme für die Notfallversorgung mit „Minimalservice" gefordert, während im White Paper darüber hinaus klare maximale Reaktionszeiten auf Störungen genannt sind.[490]

5.1.3.1.3 Basler Eigenkapitalvereinbarung

Eine der wichtigsten Säulen für bankaufsichtliche Maßnahmen zur Gewährleistung des ordnungsgemäßen Betreibens von Bankgeschäften weltweit ist die Basler Eigenkapitalvereinbarung aus dem Jahr 1988 (Basel I), die 2003 um die Neue Basler Eigenkapitalvereinbarung (Basel II) ergänzt werden soll, die dann ab 2006 in Kraft treten soll. In Basel II werden Operationelle Risiken erstmals adressiert. Die dabei gelegten Grundlagen für das Managment Operationeller Risiken sind so bedeutsam, dass sie im Zusammenhang mit der Untersuchung über die Sicherheit elektronischer Bezahlsysteme in der vorliegenden Arbeit einen breiten Raum einnehmen (siehe insbesondere Abschnitt 5.4).

5.1.3.1.3.1 Basler Eigenkapitalvereinbarung: Historie und Bedeutung

Basel I wurde 1988 verabschiedet, um grundlegenden Problemen im weltweiten Finanzgefüge zu begegnen. Zunächst hatten ‚lediglich' die Zentralbanken der Länder der Zehnergruppe[491] dieser Vereinbarung der Bankenaufsicht unter der Federführung des Basler Ausschusses für Bankenaufsicht der Bank für Internationalen Zahlungsausgleich (BIZ) zugestimmt. Das Ziel des ersten Akkords bestand in der Harmonisierung der Eigenkapital- und Liquiditätsvorschriften für Banken, da heterogene Vorschriften der verschiedenen Industrienationen zunehmend unerwünschte Regulierungsarbitrage möglich gemacht hatten.

Der Schwerpunkt der Regelungen in Basel I liegt auf einer einheitlichen Vorgabe für die Risiken aus dem Aktivgeschäft der Geschäftsbanken – 8 vH der risikogewichteten Aktiva

[489] Vgl. BIZ (2001b), S. 44 ff. und Ausführungen in Abschnitt 5.3.
[490] Vgl. 4.4.1.3.3.
[491] Die Zehnergruppe (G10) sind mittlerweile 11 Länder: die G7 Länder (USA, Japan, Kanada, Deutschland, Frankreich, Großbritannien und Italien) und zusätzlich Belgien, Niederlande, Schweden und Schweiz.

müssen für begebene Kredite mit Eigenkapital unterlegt werden. Eigenkapitalanforderungen werden in europäischer Namensgebung Eigenmittelanforderungen genannt. Dabei werden drei Formen von Eigenmitteln unterschieden: Sogenanntes „Tier 1 Capital“ ist Basis- oder Kernkapital, „Tier 2 Capital“ kann als Ergänzungskapital angerechnet werden und „Tier 3 Capital“ sind Drittrangmittel zur Deckung bestimmter Risikopositionen.[492] Der Ansatz der Eigenmittelunterlegung wurde 1989 mit der EG-Solvabilitätsrichtlinie und der EG-Eigenmittelrichtlinie in europäisches (Banken)recht übernommen. Auf nationaler Ebene fand 1993 mit der 4. KWG-Novelle eine Präzisierung der Bestimmungen zu haftenden Eigenmitteln statt. Ebenfalls 1993 wurde die Regulierung sukzessive mit der EU-Kapitaladäquanzrichtlinie auf die gesamte Finanzbranche ausgedehnt.

Die Veränderungen der Kapitalmärkte und eine Häufung von internationalen Finanzkrisen verdeutlichten im Laufe der neunziger Jahre die Notwendigkeit einer Reform von Basel I. Im Januar 2001 wurde „The New Basel Capital Accord“ (Basel II) durch den Basler Ausschuss veröffentlicht.[493] Nach voraussichtlich drei Konsultationsphasen bis Ende 2003 wird Basel II offiziell verabschiedet und soll bis Ende 2006 in den Mitgliedsstaaten umgesetzt werden.

Basel II trägt der Entwicklung an den Kapitalmärkten Rechnung und verbessert konzeptionell – bei weiter bestehenden Quantifizierungsproblemen – die bisher pauschalisierte Zuordnung von Kreditrisiko und die Unterlegung mit regulatorischem Eigenkapital.

Basel I und aller Voraussicht nach auch Basel II können als Schrittmacher der Regulierung verstanden werden. EU-Gesetze und EU-Richtlinien sollen in Zukunft mit Hilfe des Verfahrens der Komitologie vereinfacht und schneller den bankenspezifischen Regulierern wie der Bank für Internationalen Zahlungsausgleich folgen. „Unter Komitologie versteht man die Konsultation von Ausschüssen, die die Kommission bei der Verabschiedung von Durchführungsmaßnahmen zu Rechtsakten des Rates unterstützen, wobei die Durchführungsbefugnisse der Kommission übertragen wurden. Die Kommission legt diese Durchführungsmaßnahmen in Form von nachgeordneten oder abgeleiteten Rechtsakten fest.“[494]

In der geplanten Fassung soll Basel II ausschließlich für international tätige Großbanken gelten. Bereits zum gegenwärtigen Zeitpunkt zeichnet sich ab, dass die europaweite Regulierung den Anwendungskreis auch auf andere Banken und Sparkassen ausweiten wird. Der Sachverständigenrat kommt in seinem Gutachten bereits 2001 zum Schluss: „Der Wirkungsbereich der neuen Regeln geht weit über die Finanzdienstleistungsbranche hinaus. [...] Damit können die Modalitäten der Kreditvergabe unter dem neuen Regelwerk einen beträchtlichen Einfluss auf die Investitionen und den Konsum ausüben.“[495] Das Regelwerk jedoch ist äußerst komplex und führt dementsprechend immer wieder zu Diskussionen, ob der Auswirkungen der neuen Bestimmungen.

5.1.3.1.3.2 Basel II und Operationelle Risiken

Operationelle Risiken haben mit zunehmendem Verständnis für ihre Größenordnungen folgerichtig in den Verhandlungen zu Basel II eine eigenständige Bedeutung bekommen. Basel II ist auf drei tragende Säulen aufgebaut:

---

[492] Vgl. Büschgen (1998), S. 1108. Im Rahmen dieser Arbeit werden die Begriffe Eigenkapital und Eigenmittel synonym gebraucht.
[493] Vgl. BIZ (2001d) und BIZ (2001e).
[494] EU (2002). Grundlegend für das EU-Verständnis von Komitologie ist der Beschluss 87/373/EWG vom 13. Juli 1987.
[495] SVR (2001), Ziffer 85, S. 66.

Säule 1 – Mindestkapitalanforderungen (Minimum Capital Requirements),

Säule 2 – Aufsichtliches Überprüfungsverfahren (Supervisory Review of Capital Adequacy),

Säule 3 – Offenlegung (Enhancement of Market Discipline Through Disclosure).

Die einzelnen Anforderungen in den verschiedenen Säulen müssen zusammen betrachtet werden, um in ihrer Reichweite verstanden zu werden. Der spezielle Bezug zu Risiken operationeller Art findet sich in Säule 1 mit der Formulierung quantitativer Eigenkapitalanforderungen.

Operationelle Risiken müssen demnach mit Eigenkapital unterlegt werden. Generell gilt, dass die Gesamtunterlegung mit regulatorischem Eigenkapital unverändert bei 8 vH liegen soll und demzufolge andere Risiken weniger stark unterlegt werden. Neu an Basel II ist das vorgeschlagene Anreizsystem für die betroffenen Banken. Verschiedene Messverfahren, die zur Zeit in der Entwicklungs- und Testphase sind, sollen eine Quantifizierung der Operationellen Risiken ermöglichen.[496] Die Ansätze, die vom Basler Ausschuss vorgestellt werden – Basisindikatoransatz, Standardansatz und fortgeschrittener Bemessungsansatz – unterscheiden sich durch die zugrunde liegenden Techniken und dem damit verbundenen Aufwand, der für die Institute daraus resultiert. Der monetäre Anreiz für die Banken, die fortgeschrittenen Verfahren zum Einsatz zu bringen, besteht im Angebot, eine Reduktion des notwendigen Eigenkapitals für diesen Risikotyp zu erhalten. Allerdings ist noch umstritten, ob die Höhe des Anreizes ausreichend ist, um substanzielle Veränderungen beim Risikomanagement der Banken sowohl bei Operationellen Risiken als auch bei Adressausfallrisiken anzustoßen.[497] Der Basler Ausschuss hat die Notwendigkeit einer flexiblen Entwicklung und Bewertung insbesondere der fortgeschrittenen Ansätze betont und Veränderungen gegenüber den ursprünglichen Vorstellungen angekündigt[498] und teilweise auch bereits umgesetzt[499].

Die Säulen 2 und 3 beschäftigen sich in allgemeiner Form, das heißt nicht speziell auf Operationelle Risiken abzielend, mit der qualitativen Aufsicht der Eigenkapitalregeln und mit der Förderung der Marktdisziplin durch Publizitätsvorschriften. Der sogenannte Supervisory Review Process (SRP) bringt über fortlaufende Überprüfungen auch der aufsichtlichen Maßnahmen eine neue Dynamik in Prüfvorgänge und in die Beziehung von Aufsicht und Finanzinstituten.

Mit der Gestaltung der 2. Säule der Neuen Eigenkapitalvereinbarung wird deutlich, dass die Aufsichtsorgane in Zukunft mehr Einblick in das Verhältnis der Finanzinstitute von Eigenkapital zu deren Gesamtrisiko erhalten möchten. Neben der Überprüfung der angemessenen Anwendung der in Säule 1 spezifizierten Verfahren zur Ermittlung der Eigenkapitalausstattung werden in Säule 2 andere Risiken betrachtet, die über die in Säule 1 betrachteten hinaus die Risikosituation der Banken beeinflussen könnten, beispielsweise die konjunkturelle Entwicklung oder Zinsänderungsrisiken im Anlagebuch. Darüber hinaus wird die qualitative Seite der Aufsicht betont. In Zukunft soll die laufende Überprüfung der institutseigenen Verfahren und deren Qualität breiten Raum bei der Arbeit der Aufsicht einnehmen.[500] Ein

[496] Vgl. ausführlich in 5.3.2.2.
[497] Vgl. Kupiec (2001), S. 19 f. Die Diskussion ist nicht neu: Burghof (1996), S. 117 ff. verweist im Kontext der Anerkennung interner Modelle zur Berechnung von Geschäftsrisiken auf die widersprüchlichen Interessen bei Geschäftsbanken und Aufsicht zur Anwendung solcher Modelle.
[498] Vgl. BIZ (2002d).
[499] Vgl. BIZ (2003c).
[500] Vgl. BIZ (2003c), S. 11f.

erklärtes Ziel ist es, die mit Basel II angestoßene Entwicklung bankinterner Risikomanagement-Prozeduren von den Banken kontinuierlich weiterentwickeln zu lassen.[501]

Principle 1	Banks should have a process for assessing their overall capital adequacy in relation to their risk profile and a strategy for maintaining their capital levels
Principle 2	Supervisors should review and evaluate banks' internal capital adequacy assessments and strategies, as well as their ability to monitor and ensure their compliance with regulatory capital ratios. Supervisors should take appropriate supervisory action if they are not satisfied with the result of this process
Principle 3	Supervisors should expect banks to operate above the minimum regulatory capital ratios and should have the ability to require banks to hold capital in excess of the minimum
Principle 4	Supervisors should seek to intervene at an early stage to prevent capital from falling below the minimum levels required to support the risk characteristics of a particular bank and should require rapid remedial action if capital is not maintained or restored

Tabelle 7: Die vier Grundprinzipien des Supervisory Review Process gemäß Säule 2[502]

Die geplanten Publizitätsvorschriften stellen mit Einschränkungen eine neue Ausrichtung aufsichtlicher Aktivitäten dar. Der regulatorische Druck auf die Geschäftsbanken soll in diesem Ansatz weniger durch Androhung von Sanktionen aufgebaut werden, als durch den möglichen Reputationsverlust durch die Einbeziehung der Öffentlichkeit. In der ersten Fassung von Basel II war für die Operationellen Risiken auch eine Veröffentlichung aufgetretener Schadensfälle vorgesehen, die allerdings im Laufe der Konsultationsphase wieder zurückgenommen wurde. Die ursprüngliche Idee lautete:[503] „...the Committee believes that banks should publicly, and in a timely fashion, disclose detailed information about the process used to manage and control their operational risks. […] It may be possible for banks to disclose operational losses in the context of a fuller review of operational risk measurement and management."

5.1.3.2 Financial Sector Assessment Program der Weltbank und des Internationalen Währungsfonds

In eigenen Analysen kommt der IWF gegen Ende der neunziger Jahre zu dem Ergebnis, dass die Marktüberwachung (surveillance) der Finanzsysteme und insbesondere der Zahlungssysteme eine zukünftige Herausforderung für den IWF darstellt.[504] Die Notwendigkeit einer solchen Aufgabe wird – wie bereits auf nationaler Ebene – aus der Bedeutung der Stabilität der Finanzmärkte und Banksysteme für die Weltwirtschaft abgeleitet.

Das Financial Sector Assessment Program (FSAP) der Weltbank und des IWF wurde im Mai 1999 zunächst als einjähriges Pilotprojekt aufgesetzt, um systemkritische Zahlungssysteme und die Rolle der Aufsicht, insbesondere der Zentralbanken in den Mitgliedsländern, zu überprüfen. Als Prüfkriterium für den Teil des FSAP, der Zahlungssysteme zum Gegenstand

[501] Vgl. BIZ (2003d), S. 138.
[502] BIZ (2001a), S. 1f.
[503] BIZ (2001c), S. 4.
[504] Vgl. Johnson et al. (1998), S. 163 ff.

hat, wurden die von der BIZ in Kooperation mit IWF und Weltbank erarbeiteten „Core Principles for Systemically Important Payment Systems“ (CPSIPS)[505] verwendet.

Der Erfolg der ersten Untersuchungen (als einziges europäisches Land wurde 1999/2000 Irland untersucht) hat bis heute zu Neuauflagen des FSAP geführt, es werden jährlich neue Länder in den Untersuchungsplan aufgenommen. Im Ergebnis kommt Barvell zum Schluss, dass die Zahlungssysteme in den Industrienationen durch die Bemühungen insbesondere im Bereich Großzahlungsverkehr seit Beginn der neunziger Jahre äußerst robust sind. Gleichwohl ist die Dynamik im Zahlungsverkehr, auch in der Entwicklung hybrider Systeme (z. B. STEP2 der EBA), unter Sicherheitsaspekten mit Vorsicht zu beobachten. Hinzu kommt, dass die Zahlungssysteme der untersuchten Schwellen- und Entwicklungsländer vielfach gravierende Schwächen haben, die nicht in kürzester Zeit behoben sein werden.[506]

Die Bedeutung des FSAP liegt nicht in der Entwicklung ausgefeilter Methoden zur Analyse von Finanz- und Zahlungssystemen. Vielmehr wird durch die Arbeit des IWF und der Weltbank die weltweite Standardisierung im Hinblick auf die Sicherheit systemkritischer Systeme vorangetrieben. Die international besetzten Expertenteams, die vor Ort arbeiten, profitieren ebenso wie die untersuchten Länder, insbesondere Entwicklungs- und Schwellenländer, von den Untersuchungen. Mithilfe von „Macroprudential Indicators“, die im FSAP entwickelt werden, wird versucht, kritische Entwicklungen im Finanzsystem frühzeitig an allgemein verfügbaren makroökonomischen Daten zu erkennen.[507] Ein weiterer wichtiger Vorteil der supranationalen Expertentätigkeit resultiert aus der Unabhängigkeit von Weltbank und IWF von nationalen Zentralbanken. Im Rahmen des FSAP werden somit Kontrollen insbesondere derjenigen Zentralbanken möglich, die neben der Oversight-Funktion auch den Betrieb systemkritischer Zahlungssysteme selbst verantworten. Die Unabhängigkeit nationaler Zentralbanken – meist begründet in der Notwendigkeit einer starken Geldpolitik – erfährt mit dem FSAP in dieser Hinsicht ein notwendiges Korrektiv.[508]

5.1.4 Kritische Würdigung des bestehenden Instrumentariums

Die bestehenden Regelungen für die Informationssicherheit in Finanzinstituten und die Sicherheit von Bezahlsystemen im speziellen sind bis vor kurzem durch weitgehend allgemein gehaltene Aussagen gekennzeichnet. Zwar wurde im Rahmen der Verschärfung der Haftung auf Geschäftsführungsebene durch das KonTraG das Risikomanagement Ende der neunziger Jahre stärker gewichtet. Wie aber im Einzelnen ein das Gesamtsystem berücksichtigendes Risikomanagement auszusehen hat, wurde dem Markt überlassen.

Methodisch lässt sich auf supranationaler Ebene ein Übergang von quantitativen Managementvorgaben zu qualitativen Vorgaben im Sinne von „best practices“ oder „sound practices“ feststellen. Dabei wird der zunehmenden Komplexität der Bankgeschäfte Rechnung getragen, ohne dass bislang feststeht, welcher Weg im Risikomanagement der geeignetste ist, oder wie eine Überprüfung qualitativer Vorgaben in der Realität auszusehen hat.

Mit der Einführung qualitativer Normen sind Prozessanalysen und deren Qualität im Risikomanagement in den Vordergrund gerückt. In dieser Hinsicht stellen die Entwicklungen rund um Basel II und Operationelle Risken den Beginn einer neuen Ära dar. Viele Konzepte sind beim Management Operationeller Risiken auf dem Prüfstand, ein abschließendes Urteil

[505] Vgl. im Detail Abschnitt 5.1.3.1.2.
[506] Vgl. Barvell (2002), S. 16ff.
[507] Vgl. IMF (2000b).
[508] Vgl. Fabritius (2003a)

wird erst in einigen Jahren bei hinreichendem Datenbestand möglich sein. Während bisher der Aufbau von Methodenwissen in der Informationssicherheit fast vollständig den Instituten überlassen war, fängt mit Basel II die Aufsicht an, eigenes Know How zu entwickeln.

Sicher ist, dass die Bemühungen um einen internationalen Standard für den Umgang mit Operationellen Risiken im Finanzsektor viele der bisherigen Regulierungen ersetzen oder präzisierend ergänzen werden. Ebenso kann als sicher angenommen werden, dass sämtliche Maßnahmen, die im Finanzsektor im Allgemeinen und im elektronischen Zahlungsverkehr im Besonderen zur Risikobegrenzung eingeführt werden, dem Regelwerk des Managements Operationeller Risiken unterliegen werden, und diesem Werk werden folgen müssen.

Für die Sicherheitsvorgaben von hoheitlicher Regulierungsseite gilt bei elektronischen Zahlungssystemen: Großzahlungssysteme werden am stärksten reguliert. Die wichtigsten Systeme dieser Art befinden sich ohnehin in Zentralbankhand. Mit den „Core Principles for Systemically Important Payment Systems“[509] ist die internationale Standardisierung von sicherheitsrelevanten Vorgaben am weitesten fortgeschritten. Für den Bereich des Massenzahlungsverkehrs, der sich stärker in privatwirtschaftlicher Hand befindet, beginnt die Regulierung von hoheitlichen Stellen in den Bereichen, in denen diese Systeme als systemkritisch im Sinne der Lamfalussy-Kriterien gewertet werden. Teilweise greifen bei diesen Systemen auch privatwirtschaftliche Regulierungsansätze, in Deutschland beispielsweise mit den Zahlungsverkehrsabkommen im ZKA, bei denen Sicherheitsfragen jedoch nicht im Vordergrund stehen. Für die Retail-Bezahlverfahren gibt es bislang so gut wie keine regulatorischen Vorgaben auf der Ebene der Bankenaufsicht – mit Ausnahme der beginnenden Diskussion um Vorgaben für elektronisches Geld bei der EZB[510]. Die Sicherheitsvorgaben für bankbetriebene Systeme wie die GeldKarte werden auf der Betreiberebene in diesem Fall im ZKA entwickelt und durchgesetzt. Zugangsprodukte, bei denen unter Umständen Finanzinstitute keine Rolle spielen, werden bis dato nicht reguliert, respektive auf Unternehmensebene gemäß eigenen Prioritäten auf sicherheitsrelevante Fragestellungen untersucht.

Im folgenden Abschnitt wird auf ausgewählte bestehende Regularien und Normen im Risikomanagement eingegangen. Anschließend wird in Abschnitt 5.3 das Risikomanagement Operationeller Risiken nach Basel II ausführlich mit Bezug zum elektronischen Zahlungsverkehr dargestellt und diskutiert. In Abschnitt 5.3.1.4 werden speziell die unterschiedlichen Anforderungen an das Risikomanagement von Zahlungssystemen thematisiert.

5.2 Risikomanagement: Grundüberlegungen und allgemeine Ansätze

Risikomanagement ist aufwändig und wird zunehmend komplexer, gerade wenn integrative Ansätze versuchen, Risiken verschiedenster Art, beispielsweise Operationelle Risken und Marktrisiken, in einer Kennzahl zusammenzufassen.

Gleichwohl kann als Leitbild und zur Begründung der Notwendigkeit eines adäquaten Risikomanagements, das aus bankaufsichtlicher Perspektive insbesondere das Eintreten einer Bankrun-Problematik verhindern soll, das Schreiben von E. J. Smith, dem späteren Kapitän der RMS Titanic aus dem Jahr 1907 zitiert werden:[511]

„Wenn mich jemand fragt, wie ich am besten meine Erfahrungen aus 40 Jahren auf hoher See beschreiben würde, so könnte ich diese Frage lediglich mit ‚unspektakulär’ beantworten.

[509] BIZ (2001b).
[510] Vgl. EZB (2003b).
[511] Beeck (2000), S. 634.

Natürlich gab es schwere Stürme, Gewitter und Nebel, jedoch war ich nie in einen Unfall jeglicher Art verwickelt, der es wert wäre, über ihn zu berichten. Ich habe während dieser langen Zeit kaum ein Schiff in Seenot erlebt ... Ich habe weder ein Wrack gesehen, noch bin ich selbst in Seenot geraten oder habe mich sonst in einer misslichen Lage befunden, die in irgendeiner Form drohte, zum Desaster zu werden."

Obwohl Operationelle Risiken durch den vermehrten Einsatz von IT in der Bankenwelt über Jahre hinweg immer mehr an Bedeutung zugenommen hatten, wurde das Gefährdungspotenzial erst mit der „Jahr 2000"-Umstellung erstmals wahrgenommen. Im Management schien bis dahin der Eindruck vorherrschend, IT wäre eine „unspektakuläre" Hilfsgröße im Produktionsprozess der Bank und es könnte schon nichts „schief gehen". Es kann lediglich spekuliert werden, wie der Anschlag des 11. September 2001 und die anschließenden Notfallmaßnahmen ohne die umfassenden Programme der IT-Konsolidierung im Vorfeld der „Jahr 2000"-Umstellung verlaufen wären.

Risikomanagement kann im engeren und im weiteren Sinne verstanden werden.[512] Im engeren Sinne bedeutet es lediglich das operative Risikomanagement, bei dem Risikopositionen im Tagesgeschäft übernommen oder abgestoßen werden. In dieser Arbeit wird der Begriff Risikomanagement im weiteren Sinne verwendet und umfasst sowohl Risikocontrolling als auch Risikosteuerung und Risikomanagement im engeren Sinne. Unter Risikocontrolling wird die Risikoidentifikation, die Risikomessung, die strategische Risikoallokation, bei der unter anderem die Verwendung regulatorischen Eigenkapitals in verschiedenen Geschäftsfeldern bestimmt wird, und die Risikokontrolle verstanden.

5.2.1 Risikomanagement: Kosten versus Nutzen

„And in the real world, security threats are everywhere. They're not things to be avoided, they're opportunities to make money. The prize doesn't go to the company that best avoids the threats, it goes to the company that best manages the risks. (Just look at the credit card industry.)"[513]

Risikomanagement im Allgemeinen und Operationelles Risikomanagement im Besonderen sind gekennzeichnet durch den Versuch, ein optimales Kosten- respektive Nutzenverhältnis im Hinblick auf Kosten für Sicherheitsmaßnahmen und erreichte Sicherheit (die sich in sinkenden Kosten für mögliche Schäden ausdrückt) zu erzielen. Dabei spielt die notwendige Balance zwischen den beteiligten Akteuren, im Sinne des Verständnisses der mehrseitigen Sicherheit, eine besondere Rolle. Können die entstehenden Kosten für bestimmte Risikomanagement-Maßnahmen nicht in betriebswirtschaftlich kalkulierbarer Weise zwischen den Nutznießern der erhöhten Sicherheit aufgeteilt werden, kann es zu einer geringeren Sicherheitsstufe kommen. Es sei denn, es gelingt den Akteuren einseitig, ihre Interessen durchzusetzen.

Ein Beispiel für eine solche einseitige Verteilung der Risiken ist die Diskussion um die Haftung bei Betrugsfällen mit Kreditkartenzahlungen. Ist es den Kreditkartenorganisationen zunächst gelungen, die Haftung im Betrugsfall im Mail-order/Telephone-order Geschäft vertraglich fast ausschließlich auf die Händlern zu übertragen, so ist durch das BGH-Urteil vom April diese Vertragsgestaltung für unzulässig erklärt worden.[514] In beiden Fällen war der

[512] Vgl. Rudolph (2000), S. 17f.
[513] Schneier (2000), S. 398.
[514] Vgl. NWIR (2002).

Verbraucherschutz in Deutschland so stark positioniert, dass die Kunden, sofern ihnen keine betrügerische Absicht nachgewiesen werden kann, nicht haften müssen.

Die Problematik um eine angemessene Beteiligung der Akteure an den Kosten für Sicherheitsmaßnahmen durchzieht in Deutschland die Diskussion um erhöhte Sicherheitsmaßnahmen im eCommerce wie einen roten Faden. Es besteht Konsens, dass eine Grundvoraussetzung für sicheren eCommerce die Lösung der Authentifizierungsproblematik in offenen Netzen darstellt. Die Lösung dieses Problems über starke kryptographische Verfahren mit zusätzlicher Hardware ist jedoch kosten- und schulungsintensiv.

In Deutschland sind die Verbraucher über Jahrzehnte nicht offen mit den Kosten für Zahlungsverkehr konfrontiert worden, im Gegenteil die meisten Online-Banking-Angebote sind für die Endverbraucher kostenfrei. Dementsprechend unwillig reagieren die zusätzlich durch den Verbraucherschutz gut gerüsteten Verbraucher auf die Vorstellung gebührenintensiver Sicherheitsmaßnahmen – ganz zu Schweigen von Maßnahmen, die software- oder hardwareseitige Installationen erfordern.

Auf der Händlerseite hat sich mit den Gebühren für Kreditkartenzahlungen offensichtlich eine Obergrenze herausgebildet, die der Handel noch akzeptieren kann. Zusätzlich kommt es im Rahmen des sogenannten „liability shifts“, bei dem die Haftung vom Händler auf die Bank übergeht, wenn bestimmte technische Maßnahmen bei der Kreditkartenabwicklung implementiert sind, zu einer risikomindernden Situation beim Händler. In der Folge werden, unter Umständen durch regulatorische Bemühungen verstärkt, die Kosten für mehr Sicherheit den Finanzinstituten aufgebürdet.

In erster Linie werden Maßnahmen im Bereich des Risikomanagements in den meisten Unternehmen als Kostenblock verstanden. Je höher die Sicherheitsanforderungen werden, umso größer werden auch die Kosten. In Abbildung 14 wird der Nutzen, verstanden als Maß an erreichter Operationeller Sicherheit, gegen die Kosten abgetragen. Dabei steigen die Kosten für Sicherheitsmaßnahmen mit höheren Sicherheitsanforderungen, die Kosten durch entstehende Schäden sinken in Abhängigkeit des erreichten Sicherheitsniveaus. Im Optimum ist die Summe beider Kostenarten minimiert. Eine Darstellung, die intuitiv erfassbar, in der Praxis jedoch äußerst schwierig mit Zahlen zu unterlegen ist. Die Kosten für zusätzliche Sicherungsmaßnahmen lassen sich gegebenenfalls erheben, die Schwierigkeiten liegen auf der Schadensseite. Werden nur tatsächlich entstandene Kosten gerechnet, wird mit Eintrittswahrscheinlichkeiten gerechnet, wie lässt sich ein potenzieller Imageschaden für das Unternehmen beziffern etc.?

Wird in einer zeitlichen Betrachtung am Anfang an Sicherheitsmaßnahmen gespart, steigen unter Umständen die Kosten für nachträgliche Implementierungen erheblich.[515] Die Kostenkurve für Sicherheitsmaßnahmen wird wie in Abbildung 23 nach links oben verschoben (KS2). In der Folge steigen die Gesamtkosten in einem Unternehmen, das versucht, die Sicherheit im nachhinein zu erhöhen, gegenüber dem präventiven Modell deutlich. Unter Umständen wird demnach bei höheren Kosten ein niedrigeres Sicherheitsmaß ($S2<S1$, $K2>K1$) erreicht. Nach Power investieren trotzdem einige Unternehmen zu wenig in ihr Risikomanagement:

„The amount of financial transactions occuring electronically has grown exponentially over the past decade. As organizations race to create e-commerce systems so they do not miss the

[515] Vgl. BSI (1999a), S. 2.

perceived band-wagon, they often create applications that have poor and, sadly, often no security built into the systems architecture and procedural controls […]. I have heard too many organizations say that they will add security 'later' after implementation so they can meet their target dates, and the later never comes."[516]

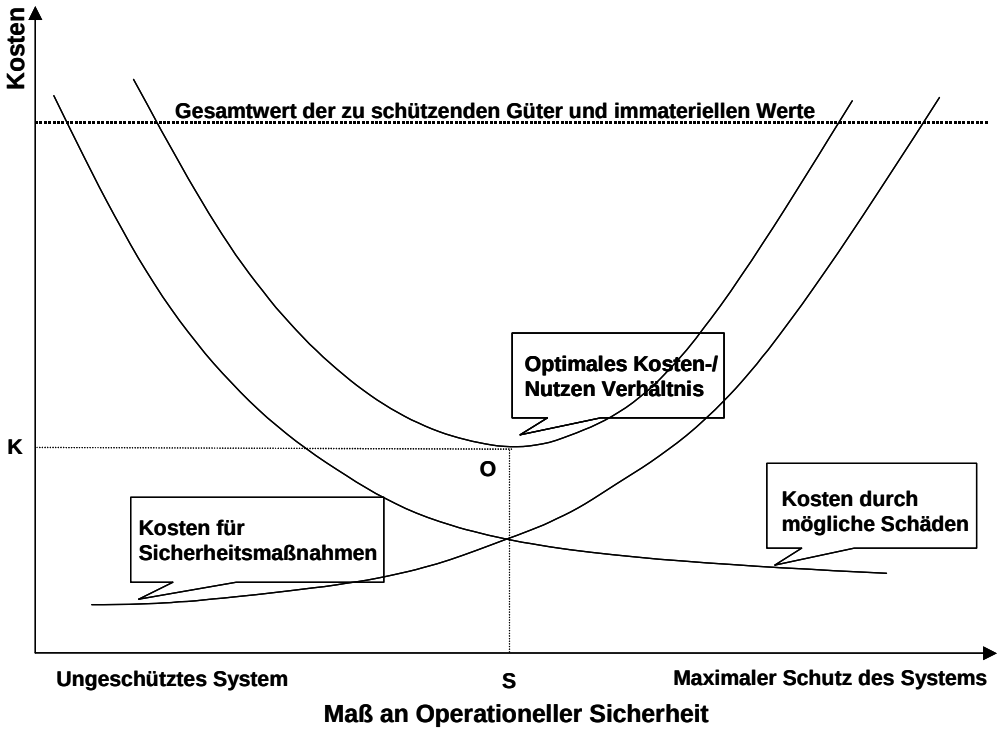

Abbildung 22: Risikomanagement: Verhältnis von Kosten zu Nutzen[517]

Als Beispiel für diese Schwierigkeiten, Sicherheit nachträglich in ein existierendes Gesamtsystem einzubauen, beschreiben Bond und Zielinski in ihrer Arbeit die Angriffsmöglichkeiten auf die PIN-Überprüfungsmodule beim Einsatz von Bank- und Kreditkarten am Geldausgabeautomaten.[518] Ihrer Ansicht nach gibt es gegen die aufgeführten Angriffe auf Geldautomaten keine schnelle, kostengünstige Lösung. Die verwendete Software wurde unter dem Eindruck eingesetzt, sie würde nie Probleme mit sich bringen, und die eingebaute Sicherheit wäre für die Lebensdauer der Geräte hinreichend hoch. Nachdem sich herausgestellt hat, dass diese Annahme falsch ist, steigt der Aufwand für eine neue, sichere Lösung exponentiell.

[516] Power (2002), S. 14.
[517] In Anlehnung an Raepple (1998), S. 9.
[518] Vgl. Bond (2003).

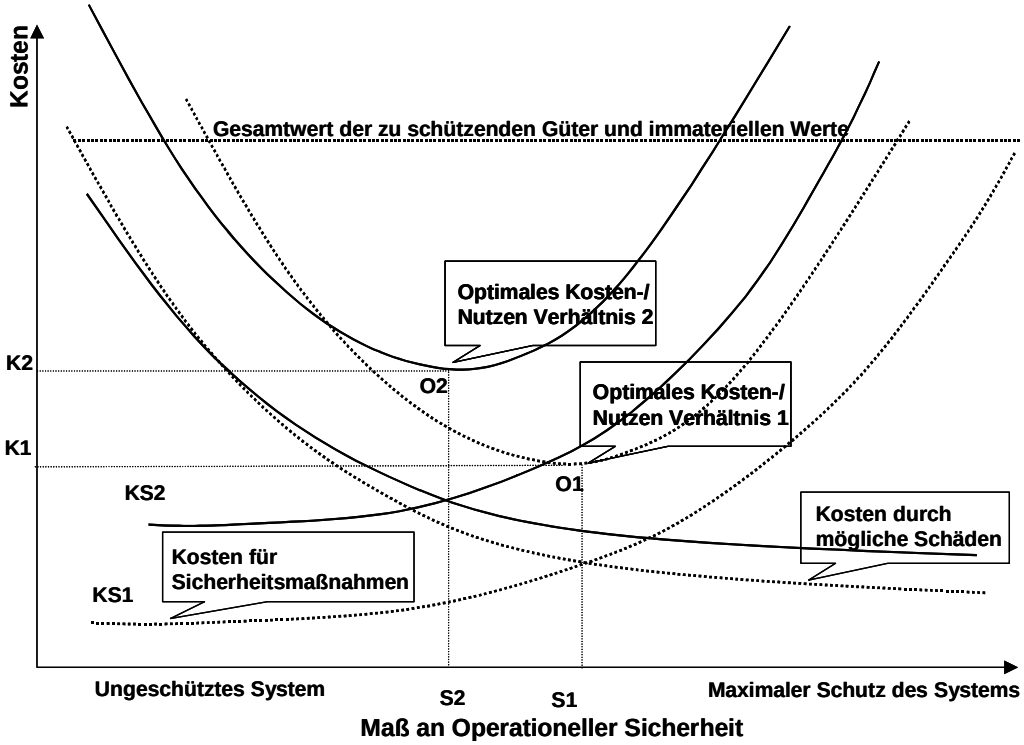

Abbildung 23: Nachträgliches Risikomanagement: Verhältnis von Kosten zu Nutzen[519]

McDonough bringt diese Erkenntnis und die notwendige Schlussfolgerung in der Position der Federal Reserve Bank of New York für den Zahlungsverkehr auf den Punkt:[520] „a gram of prevention is worth a kilogram of cure".

5.2.2 Risikomanagement: der Prozess

„The error of Applied Cryptography is that I didn't talk at all about the context. I talked about cryptography as if it were The Answer™. I was pretty naiv.....Security is not a product; it itself is a process. And if we're ever going to make our digital systems secure, we're going to have to start building processes. [...] If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."[521]

Für jedes Risikomanagement, sei es IT-Risikomanagement oder das Management Operationeller Risiken gilt ein grundsätzlicher Zyklus, der sich als Standard beim Risikomanagementprozess etabliert hat[522] (siehe Abbildung 24).

[519] Eigene Darstellung.
[520] McDonough (1998), S. 15.
[521] Schneier, B. (2000), S. xii.
[522] Vgl. u.a. KPMG (1998), BMÖLS (1998), BSI (1999b).

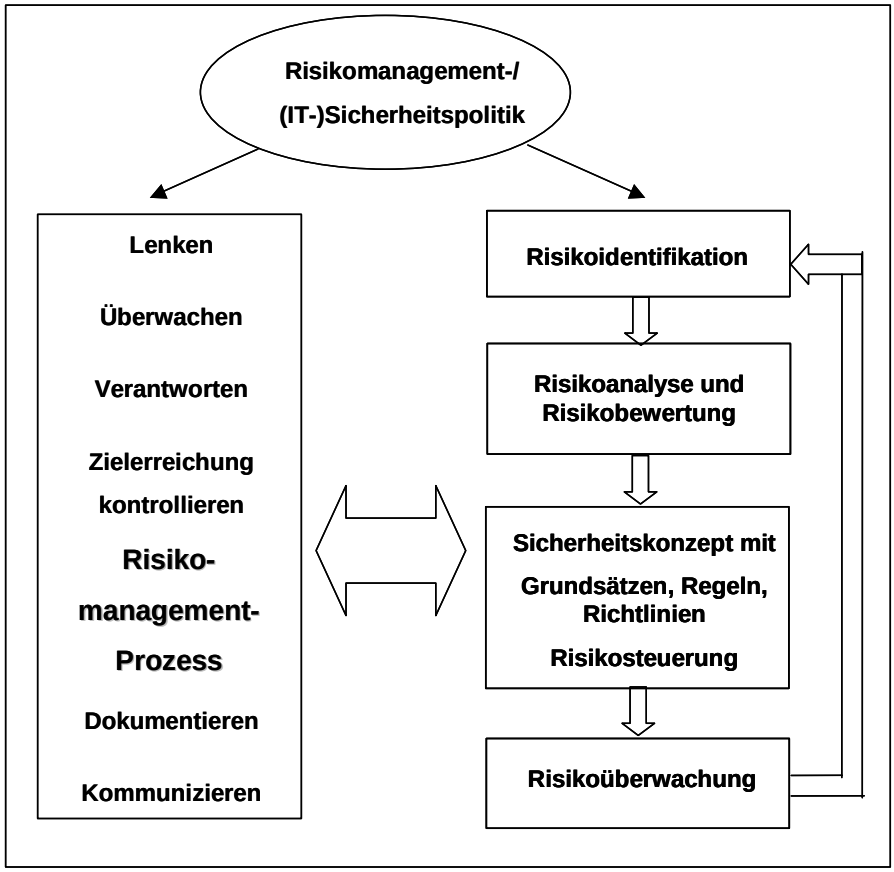

Abbildung 24: Der Risikomanagementprozess[523]

Die einzelnen Phasen des Risikomanagementprozesses sind zunächst das Festlegen einer Sicherheitspolitik, dann auf der operativen Ebene die Risikoidentifikation, die Risikoanalyse und -bewertung, die Risikosteuerung und die Risikoüberwachung.

Zentrale Bedeutung beim Risikomanagement hat in jeder Unternehmung die Formulierung der unternehmensweiten Risikomanagement- oder Sicherheitspolitik mit entsprechender Verankerung dieses Vorhabens auf höchster Unternehmensebene. Es werden Leitlinien und Vorgaben schriftlich fixiert, die wesentliche Ziele, Strategien aber auch Methoden zur Erreichung der Gesamtziele festlegen.

Erst aufgrund einer sorgfältigen unternehmensweiten Identifikation, Analyse und anschließenden Bewertung der möglichen Risiken, denen ein Unternehmen ausgesetzt ist, kann eine Organisation sich mit dem Konzept auseinandersetzen, wie mit diesen Risiken umgegangen werden soll und kann. Grundsätzlich lassen sich vier Strategien der Risikosteuerung unterscheiden (siehe Abbildung 25). Die ersten beiden Strategien, „Vermeiden von Risiken“ und „Vermindern von Risiken“ stehen dabei im Mittelpunkt des Interesses, zumindest solange von einer kostengünstigeren Umsetzung ausgegangen wird als in den beiden letzten Strategien, die bedeuten, Risiken gegen Entgelt auf Dritte abzuwälzen oder das (Rest-)Risiko selbst zu tragen.

[523] In Anlehnung an KPMG (1998), S. 16, BMÖLS (1998), S. 9., BSI (1999b), S. 2.

Risiko...			
...vermeiden durch:	**...vermindern durch:**	**...überwälzen auf:**	**...selbst tragen:**
u.a. organisatorische Maßnahmen, Sicherung von Zugriffsrechten und Zugang, Personalüberprüfung, Aufbau gezielter Redundanzen	u.a. Eskalationspläne, Notfallpläne, regelmäßige Überprüfung, Krisenstäbe, Personaltraining, -schulung, organisatorische Maßnahmen	Versicherungen, Dienstleister (Outsourcing)	Restrisiko

Abbildung 25: Risikosteuerung: Strategien zum Umgang mit Risiko[524]

Risiko zu vermeiden, kann in der extremsten Ausprägung bedeuten, aufgrund einer Neubewertung der Risikosituation zum Schluss zu kommen, einzelne Aktivitäten innerhalb der Unternehmung einzustellen, beispielsweise ein Produkt nicht mehr zu produzieren, oder eine Produktionsstätte zu schließen.

Risikoverminderung hat zum Ziel, die Summe der Produkte von Eintrittswahrscheinlichkeit und Schadenshöhe einzelner identifizierter Risiken zu minimieren. Technische und organisatorische Änderungen der Abläufe, von Organisationseinheiten etc. stehen dabei an erster Stelle der Maßnahmen, um dieses Ziel zu erreichen.

Im Rahmen der Diskussion im Verlauf der Konsultationen zu Basel II hat sich die Schwierigkeit bei der Strategie des Überwälzens von Risiken auf Dritte gezeigt. Versicherungen für Schadensfälle durch Operationelle Risiken sollten zunächst überhaupt nicht anrechenbar sein. Nach der dritten Konsultationsphase wird den Unternehmen, die die fortgeschrittensten Ansätze zur Messung des Operationellen Risikos verwenden, zugestanden, bis zu 20 % ihrer Operationellen Risiken durch Versicherungen abzudecken und damit die Unterlegung mit regulatorischem Eigenkapital zu reduzieren.[525]

Für die restlichen Risiken, einerseits die so genannten Restrisiken, andererseits die Risiken, die ein Unternehmen als gering genug erachtet, um sie problemlos tragen zu können, bleibt als Strategie die Übernahme durch das eigene Unternehmen übrig. Diese Strategie kann auch dann betriebswirtschaftlich sinnvoll sein, wenn es beispielsweise dem Unternehmen nicht gelingt, ein geringes Risiko einem Dritten als gering zu vermitteln. In der Folge könnte eine Risikoprämie unverhältnismäßig hoch sein, und die eigene Übernahme des Risikos die optimale Strategie darstellen.

Die Risikoüberwachung soll gewährleisten, dass die genannten Strategiealternativen der Risikosteuerung zielgerichtet umgesetzt werden. Letztlich ist Ziel der Risikoüberwachung, den Risiko-Ist-Zustand mit dem Risiko-Soll-Zustand abzugleichen. Diese Aufgabe kann nur mit Hilfe eines ausgereiften Informations- und Berichtsystems erreicht werden.

Das ordnungsgemäße Funktionieren des Risikomanagement-Systems muss auf allen Einzelstufen kontinuierlich überwacht werden. Im Falle von Abweichungen, deren Ursachen

[524] Eigene Darstellung, Kategorisierung in Anlehnung an Saitz (1998), S. 78ff.
[525] Vgl. BIZ (2003c), S. 21 Ziffer 92.

unternehmensintern bedingt sein können, aber auch in äußeren Einflüssen auf das Unternehmen liegen können, muss das System nachjustiert werden können. Dies gilt ebenfalls für Optimierungsprozesse, die intern oder extern entwickelt werden. Die Leistungsfähigkeit eines Risikomanagement-Systems zeigt sich einerseits bei der Fähigkeit, die einzelnen Prozesse effektiv umzusetzen, andererseits bei der Geschwindigkeit, mit der Änderungen im System umgesetzt werden können.

Im folgenden werden die international gebräuchlichsten Standards vorrangig aus dem Bereich des IT-Sicherheitsmanagements, das von der Intention dem Management Operationeller Risiken am nächsten kommt, mit ihren jeweiligen Umsetzungmaßnahmen beschrieben: der technische Bericht ISO/IEC 13335, das Grundschutzhandbuch des BSI und die Norm ISO/IEC 17799.

Im eigentlichen Wortsinn ist selbst der aktuellste internationale Standard ISO 17799, der aus dem British Standard 7799 hervorgegangen ist, kein Standard, der für eine umfassende Berücksichtigung Operationeller Risiken konzipiert wurde. Einen solchen Standard gibt es industrieweit bisher nicht, insofern ist es gerechtfertigt, im Rahmen dieser Arbeit Ansätze vorzustellen, die dem „Idealtyp“ eines Operationellen Risikomanagements konzeptionell möglichst nahe kommen. In der Ausgestaltung der Anforderungen an ein Operational Risk Management hat sich die BIZ insbesondere am ISO/IEC 17799 orientiert.

5.2.3 Organisatorische Sicherheit im IT-Sicherheitsmanagement: Branchenunspezifische Ansätze

Die wachsende Abhängigkeit der meisten Unternehmen von Informationstechnologien hat die Einführung von IT- Sicherheitsmanagementsystemen, die neben technischen auch organisatorische Risiken und Sicherheitsmaßnahmen berücksichtigen, unerlässlich gemacht.

Elektronische Zahlungssysteme sind hochschutzbedürftige IT-Systeme, die eine detaillierte Risikoanalyse erfordern. Eine Grundschutzanalyse beispielsweise auf Basis des Grundschutzhandbuchs des BSI,branchenunabhängig konzipiert, reicht dazu nicht aus, sondern kann lediglich als Startpunkt dienen. Es ist erforderlich, die speziellen Risiken der Branche sowohl technischer, als auch organisatorischer Art zu identifizieren und geeignete Maßnahmen zu deren Bewältigung zu implementieren. Gleichwohl sichert eine Analyse nach Grundschutzhandbuch ein einheitliches Niveau für die Gesamtunternehmung, von dem ausgehend weitere vertiefende Untersuchungen geprüft werden können.

In den neunziger Jahren ist der Bereich Sicherheitsmanagement auf die Informationstechnologie konzentriert, auf der technischen Ebene dominieren die Common Criteria, weitere Bezüge auch zu personellen und organisatorischen Aspekten stellen unter anderem das IT-Grundschutzhandbuch, das IT-Sicherheitshandbuch für die öffentliche Verwaltung (Österreich) und die „Information Technology – Guidelines for the Management of IT Security (ISO/IEC 13335) dar. Gegen Ende der neunziger Jahre rücken vermehrt Fragestellungen der Informationssicherheit im weiteren Sinne (siehe Abbildung 26) und organisatorische Belange in den Vordergrund und finden ihren Niederschlag im British Standard 7799, der schließlich als ISO/IEC 17799 internationalisiert wird.

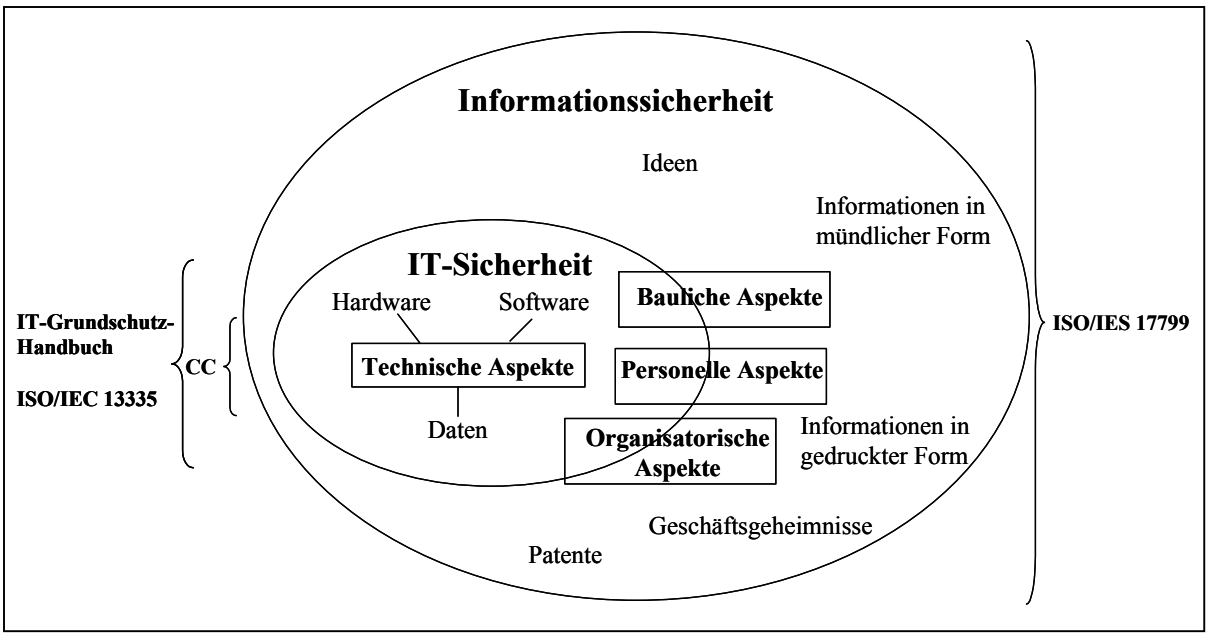

Abbildung 26: IT-Sicherheit als Teilbereich der Informationssicherheit und relevante Management-Normen[526]

Bereits in der Zielsetzung der einzelnen Ansätze ergeben sich Unterschiede. Der Fokus von ISO/IEC 13335 liegt auf der Etablierung eines Managements für IT-Sicherheit und formuliert Managementmaßnahmen. Dahingegen konzentriert sich das Grundschutzhandbuch darauf, geeignete Sicherheitsmaßnahmen für typische IT-Systeme zu finden und sehr detailliert und häufig aktualisiert spezifische Maßnahmen vorzugeben. Die ISO Norm 17799 hat zum Ziel, für Unternehmen jeder Größe und aller Branchen eine Grundlage des sicheren Informationsmanagements zu bilden – eine gemeinsame Basis zur Entwicklung von organisationsbezogenen Sicherheitsnormen und effektiven Sicherheitsmanagementpraktiken soll gebildet werden.

Generell zeichnen sich die branchenunspezifischen Ansätze durch ihren generischen Ansatz aus, das heißt, sie gehen nicht so sehr ins ausgestaltende Detail, sondern versuchen vielmehr systematisch die Grundlagen für einen Sicherheitsmanagement-Prozess zu legen. In der Praxis muss dann versucht werden, die branchenspezifische Umsetzung voranzutreiben. Das Grundschutzhandbuch stellt hier eine gewisse Ausnahme dar. Wie der Name sagt, ist der Grundschutz das eigentliche Ziel, mit dem Resultat, dass allgemeine Systemeigenschaften detailliert überprüft werden können, da beispielsweise ein Windows-Betriebssystem quer über alle Branchen eingesetzt wird. Für branchenspezifische Fragen ist das Grundschutzhandbuch nicht konzipiert.

Für Finanzinstitute können dabei die Arbeiten der BIZ im Hinblick auf Basel II als weit fortgeschritten bezeichnet werden – Grundlage bilden die „Sound Practices for the Management and Supervision of Operational Risk“. Probleme zeigen sich allerdings im Detail der Umsetzung und in der aufsichtlichen Überprüfbarkeit (siehe Abschnitt 5.3).

5.2.3.1 BSI Grundschutzhandbuch

Der IT-Sicherheitsprozess, der von der Erstellung von IT-Sicherheitsrichtlinien über die Einrichtung eines Sicherheitsmanagements bis hin zur Erstellung und Umsetzung eines IT-Sicherheitskonzeptes und die Umsetzung im laufenden Betrieb reicht, wird im Grundschutzhandbuch adressiert. Insbesondere die Konzeption des IT-Sicherheitskonzeptes nimmt im Grundschutzhandbuch breiten Raum ein (vgl. Abbildung 27).

[526] In Anlehnung an Niemann (2001), S. 6.

Das Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI)[527] konzentriert sich auf typische IT-Systeme wie Linux oder Windows mit den unterschiedlichen Ausprägungen und kann dadurch sehr ins Detail gehen. Es werden Maßnahmenkataloge verwendet, um die Sicherheit der IT-Systeme, die in Bausteinen abgebildet wird, zu gewährleisten. Jeder Baustein behandelt ein spezifisches sicherheitsrelevantes Thema oder System, beispielsweise einzelne Betriebssysteme oder das Thema Internetzugang, und wird systematisch nach typischen Gefährdungen (höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen) und geeigneten Gegenmaßnahmen (Infrastruktur, Organisation, Personal, Hardware/Software, Kommunikation und Notfallvorsorge) aufbereitet. Die im Anschluss an eine IT-Grundschutzanalyse erforderliche Umsetzung für das Unternehmen kann in der Folge mit deutlich weniger Aufwand realisiert werden, als dies bei einer detaillierten firmenspezifischen Risikoanalyse der Fall wäre.

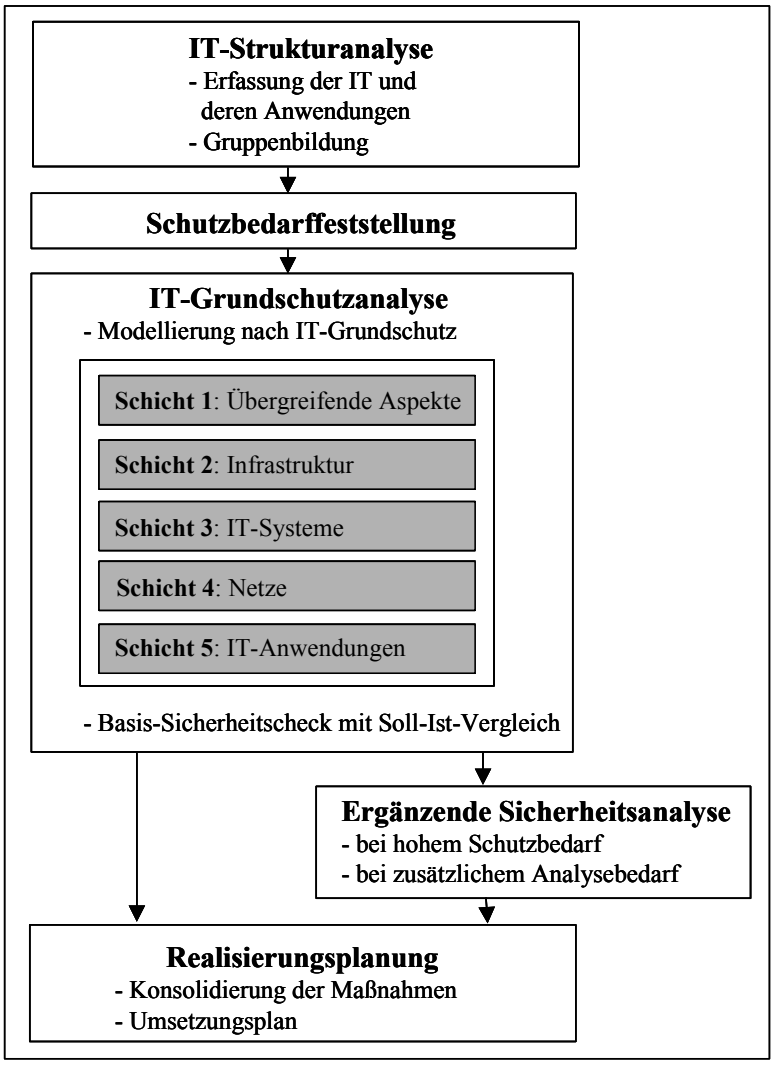

Abbildung 27: IT-Grundschutzhandbuch des BSI: Erstellung eines IT-Sicherheitskonzepts[528]

[527] Vgl. BSI (2000).
[528] Eigene Darstellung in enger Anlehnung an BSI (2000), S. 3, S. 27.

Das Grundschutzhandbuch weist darauf hin, dass für IT-Systeme, die sich nicht auf die vorgeschlagenen Bausteine abbilden lassen, oder die einen höheren Schutzbedarf haben, ergänzende IT-Sicherheitsanalysen notwendig sind. Diese sind aber nicht Gegenstand des Grundschutzhandbuchs. Dennoch bilden die Standardsicherheitsmaßnahmen des Grundschutzhandbuchs eine gute Sicherheitsbasis für hochschutzbedürftige IT-Systeme und schaffen zumindest eine einheitliche Grundlage, auf die vertiefend aufgebaut werden kann. Bei der Anwendung in sicherheitsrelevanten Umgebungen, wie beispielsweise dem Finanzsektor, erweist sich die sektorübergreifende Auslegung des Grundschutzhandbuchs in gewisser Hinsicht als Schwäche.[529] Es können keine branchenspezifischen Vorgaben berücksichtigt werden. Dadurch wird unter Umständen der Einsatz des Grundschutzhandbuchs für einzelne Sektoren uninteressant, insbesondere wenn diese der Meinung sind, ihre Anforderungen wären ohnehin höher als die des Grundschutzes.

Da das Grundschutzhandbuch auf spezifische IT-Produkte (wie z. B. in Maßnahme M 4.55: Sichere Installation von Windows NT) eingeht, besteht die Gefahr, dass es schnell altert und laufend neue, dem Stand der Technik angepasste Maßnahmen der Standardsicherheit entwickelt werden müssen. Das Grundschutzhandbuch unterliegt in der Folge genau wie die einzelnen IT-Sicherheitskonzepte der Unternehmen einer ständigen Überarbeitung. Das BSI garantiert dabei die Qualität und Aktualität der Standardsicherheitsmaßnahmen und greift zur Erweiterung einzelner Module auf externes Beraterwissen zurück.

5.2.3.2 ISO/IEC 13335

Die ISO/IEC 13335 Norm „Information Technology – Guidelines for the Management of IT Security“ ist als Technischer Report konzipiert und besteht aus fünf Teilen. Sie bietet ein ganzheitliches IT-Sicherheitsmanagement, das mit der Konzeptionierung und Modellierung in Teil 1 beginnt und bis hin zu Sicherheitsmaßnahmen bei Anbindung an offene Netzwerke in Teil 5 geht. Jeder durchzuführende Schritt ist beschrieben, und auf eventuelle Probleme, die auftreten können oder Besonderheiten wird gezielt hingewiesen.[530] Dabei bestehen immer Rückkoppelungen zwischen den verschiedenen Phasen, um eventuelle Fehler auch im nachhinein korrigieren zu können. Es wird darauf Wert gelegt, dass die Erstellung eines IT-Sicherheitsmanagements kein einmaliger Prozess ist, sondern kontinuierlich überwacht und aktualisiert wird. Dazu tragen verschiedene Methoden, die im laufenden Betrieb eingesetzt werden bei, z. B. das Security Compliance Checking (Überprüfungsverfahren, ob Vorgaben eingehalten werden) oder das Change Management, mit dessen Hilfe sicherheitsrelevante Änderungen flexibel im Unternehmen umgesetzt werden sollen.

ISO/IEC 13335 schlägt ein kombiniertes Verfahren vor, das eine detaillierte Risikoanalyse für hochschutzbedürftige und eine Grundschutzanalyse für alle anderen IT-Systeme vorsieht. So wird ein angemessenes Sicherheitsniveau für das Unternehmen garantiert, wobei der größere Aufwand für hochschutzbedürftige IT-Systeme anfällt.

Probleme könnten bei der Wahl des Sicherheitsmanagement-Teams entstehen, denn um eine detaillierte Analyse durchführen zu können, ist sowohl ein sehr gutes Verständnis der eingesetzten IT-Systeme und des heutigen Stands der Technik als auch Erfahrung mit IT-Sicherheitsfragen notwendig. Der Rückgriff auf externe Berater erscheint an dieser Stelle unverzichtbar.

[529] Vgl. Münch (2002), S. 39 f.
[530] Vgl. ISO/IEC TR 13335 Teile 1 bis 5.

ISO/IEC 13335 und das Grundschutzhandbuch ergänzen sich. So empfiehlt beispielsweise ISO/IEC 13335 Teil 3 die Anwendung einer Grundschutzanalyse, falls es sich nicht um hochschutzbedürftige IT-Systeme handelt. Das Grundschutzhandbuch hingegen nennt zur Konzeption und Erstellung eines IT-Sicherheitsmanagements als weiterführende Literatur die Richtlinien des ISO/IEC 13335.

5.2.3.3 ISO/IEC 17799

Die ISO/IEC 17799 Norm behandelt Fragen der IT-Sicherheit umfassender – im Sinne des erweiterten Sicherheitsbegriffs – als im Grundschutzhandbuch und der ISO/IEC 13335 Norm. Es wird nicht auf ein spezifisches Verfahren zur Erstellung eines IT-Sicherheitsmanagement verwiesen, sondern eine Sammlung von Sicherheitsmaßnahmen vorgeschlagen, die insbesondere aus dem Bereich der Organisation kommen. Bemerkenswert ist, dass selbst in Bereichen, wie z. B. der Systementwicklung und –wartung, in denen bei den anderen zwei Konzepten technische Maßnahmen überwiegen, die ISO/IEC 17799 Empfehlungen für organisationsbezogene Sicherheitsnormen gibt; diese werden sogar in den Vordergrund gestellt. So entsteht der Eindruck, die Technik diene nur als Hilfsmittel zur Umsetzung der organisatorischen Anforderungen. Da die ISO/IEC 17799 als Grundlage zur IT-Sicherheit für Unternehmen jeder Größe und aller Branchen dienen soll, werden diese organisatorischen Sicherheitsfragen sehr allgemein angesprochen und keine konkreten Lösungsvorschläge gegeben. Jedoch kann gerade die Umsetzung dieser allgemeinen Anforderungen sehr komplex werden. Hinzu kommt, dass der Aufbau der Norm nicht erläutert wird und keine Priorisierungsanleitung gegeben wird. Daher ist es für Unternehmensverantwortliche schwierig nachzuvollziehen, was in welcher Reihenfolge zu beachten ist. Es bleibt offen, welche organisatorischen Sicherheitsmaßnahmen unabdingbar und welche optional sind.

Sind die Ressourcen des Unternehmens beschränkt, so stellt sich die Frage, welche Sicherheitsmaßnahmen der Norm umgesetzt werden müssen, um den eigenen Sicherheitsanforderungen gerecht zu werden und welche weniger wichtig sind. Auf die Bedeutung einer Risikoanalyse wird zwar hingewiesen und diese auch kurz definiert, dennoch ist weder erläutert, wie genau vorzugehen ist, noch welcher Zusammenhang zwischen Risikoanalyse und den von ISO/IEC 17799 vorgeschlagenen Maßnahmen besteht. Wird keine Risikoanalyse durchgeführt, so weiß das Unternehmen nicht, welchen Risiken es ausgesetzt ist. Folglich ist nicht klar, welche Sicherheitsmaßnahmen umgesetzt werden müssen. Auch das verbleibende Restrisiko nach Implementierung der von der ISO/IEC 17799 Norm vorgeschlagenen Maßnahmen, bleibt dem Unternehmen unbekannt. Es stellt sich also die Frage, ob man ein Unternehmen, das die Maßnahmen der Norm umsetzt, ohne eine angemessene Risikoanalyse durchzuführen, als sicher bezeichnen kann.

Die Bedeutung dieser Norm ist dennoch nicht zu unterschätzen, da sie die einzige ist, die den Schwerpunkt auf die Organisation im Sicherheitsmanagement legt. Zudem kristallisiert sich die ISO 17799 als „best practice“-Vorgabe im Risikomanagement Operationeller Risiken heraus und stellt damit eine wesentliche Grundlage für das Management Operationeller Risiken im Finanzsektor dar.

5.3 Management Operationeller Risiken bei Banken: Darstellung und weiterführende Überlegungen anhand Basel II

„If we haven't seen widespread fraud agaist Internet payment systems yet, it's because there isn't a lot of money to be made there yet. When there is, criminals will be there trying. And if history is any guide, they will succeed."[531]

Die Bedrohungen, denen der elektronische Zahlungsverkehr ausgesetzt ist, sind fast vollständig der Klasse der Operationellen Risiken zuzuordnen. Sonstige denkbare Schadensfälle wären eventuell bei strategischen Risiken anzusiedeln, beispielsweise die Wahl eines technisch nicht leistungsfähigen Systems, oder die fehlerhafte Entscheidung zugunsten eines im Wettbewerb unterlegenen Zahlungsverkehrssystems.

5.3.1 Operational Risk Management: der Prozess

5.3.1.1 Operational Risk Management als prozessorientierter Ansatz

In Abschnitt 2.6 und den folgenden Beispielen wird deutlich, dass elektronische Abwicklungen in der Finanzbranche, insbesondere im elektronischen Zahlungsverkehr, erheblichen Risiken ausgesetzt sind.[532] Allerdings sind die bestehenden Regulierungen und die bankinternen Prozeduren (noch) nicht im notwendigen Maße auf ein durchgängiges Risikomanagement Operationeller Risiken ausgerichtet.

Ende der neunziger Jahre wurde dieses Problem auf internationaler Ebene erkannt und in die Verhandlungen zur Neuen Basler Eigenkapitalvereinbarung eingebracht. In Abschnitt 5.2.3 wurde deutlich, dass die branchenunspezifischen Ansätze zwar in internationale Normen und nationale Maßnahmen umgesetzt wurden, aber noch keine Branche sich tatsächlich auf die geprüfte Umsetzung dieser Normen und Maßnahmen beruft.

In diesem Abschnitt wird dargestellt, welchen eigenständigen Weg, aufsichtlich motiviert, die Finanzbranche im Umfeld des Operational Risk Managements geht. Dabei wird auf die Bedeutung der in Basel II vorgesehenen Prozeduren und Managementvorschriften aber auch auf die Probleme bei der Erfassung Operationeller Risiken, nicht nur im Zahlungsverkehr, eingegangen.

Weitgehend ungeklärt ist, ob es den aufsichtlichen Instanzen gelingt, ihre Prüfprozeduren so auszurichten, dass das Operational Risk Management tatsächlich innerhalb der Banken zu erheblichen Verbesserungen führt und nicht lediglich mit verschiedenen Ansätzen versucht wird, Vergleichszahlen, die aufsichtlichen Gesichtspunkten genügen, zu produzieren.

War bis vor wenigen Jahren der Zahlungssystem-Markt fast ausschließlich in Bankenkontrolle, entwickelt sich dieser Markt, wie bei der Diskussion der strategischen Positionen der Akteure im Zahlungsverkehr in Abschnitt 4.2.6.5 aufgezeigt, in Richtung Konsumenten, aber auch im B2B-Bereich aus der Bankenwelt hinaus. Neben den Telekommunikationsunternehmen bieten weitere Dienstleister wie die Firstgate Internet AG und die Bibit Internetzahlungen GmbH Zahlungssysteme und Zahlungssystem-Dienstleistungen an. Noch existieren erhebliche Markteintrittsbarrieren für außereuropäische Finanzdienstleister, durch Zukäufe können und konnten diese aber partiell überwunden werden. Ein Beispiel liefert der Erwerb der Telecash GmbH, Marktführer in Deutschland für die Abwicklung von Maestro-Zahlungen

[531] Vgl. Schneier (2000), S. 16.
[532] Vgl. Abschnitt 5.3.2.1.

und Kreditkartenzahlungen, durch die amerikanische Firma FirstData Corporation im Februar 2003.[533] Es scheint nur noch eine Frage der Zeit, bis andere Akteure, beispielsweise Internet-Dienstleister aber auch Telekommunikationsfirmen, die das UMTS-Debakel finanziell verkraftet haben und neue Geschäftsfelder suchen, eine Banklizenz anstreben.

Die komplexeren Strukturen erschweren in Verbindung mit der Anzahl beteiligter Akteure eine durchgängige prozesshafte Betrachtung des Zahlungsverkehrs unter Sicherheitsaspekten. Zusätzlich kann das bisherige, lange Jahre geübte, Aufsichts- und Kontrollgefüge empfindlich gestört werden, da ein wachsender Anteil an Dienstleistern nicht ausschließlich für den Finanzsektor arbeitet und somit dessen etablierten Sicherheitsregelsystemen nicht angehört. Operational Risk Management ist der Versuch, Sicherheit nicht mehr als Produkt, sondern als Gesamtprozess zu sehen und entsprechend zu behandeln. Dies hört sich zunächst einfach und nachvollziehbar an, bringt aber in der Umsetzung erhebliche Probleme mit sich.

Aus dieser Argumentation heraus lassen sich auch Bemerkungen von IT-Sicherheitsexperten verstehen. Etwa Ross Anderson, der die technische Überbetonung von Sicherheitsfragen kritisiert: [534]
„There are many more mathematicians active in security research than applied psychologists, and it shows."

Er stellt weiter in Hinblick auf wirkungsvolle Risikomanagement-Methoden fest:[535]
"When it comes to developing robust management controls and business processes that limit the amount of damage that any one staff member can do, there is a striking lack of hard material (especially given the need that new e-businesses have for such systems)."

Den Betrug in kleinem und großem Stil im, mit und ohne Internet wirkungsvoll zu bekämpfen, würde nach Ansicht vieler Experten ein konzertiertes Vorgehen erfordern. An erster Stelle würde dabei nach Ansicht der US National Security Agency das Bemühen der Hersteller um sichere Betriebssysteme als Grundlage des eCommerce zu stehen haben:[536]
„The computer industry has not accepted the critical role of the operating system to security, as evidenced by the inadequacies of the basic protection mechanisms provided by current mainstream operating systems. The threats posed by the modern computing environment cannot be addressed without secure operating systems. Any security effort which ignores this fact can only result in a 'fortress built upon sand'."

Auch Arnfield kommt in seiner Analyse zum Schluss, dass alle Beteiligten im eCommerce-Segment ein gemeinsames Interesse an sicheren Anwendungen haben müssten. Er leitet aus den Sicherheitsbedürfnissen die Notwendigkeit eines konzertierten Vorgehens aller Akteure, insbesondere Banken, Kreditkartenunternehmen, Telefongesellschaften, Internet Service Providern und Soft- und Hardwareentwicklern ab.[537]

Die Ansätze für ein Operational Risk Management im Rahmen von Basel II akzeptieren zunächst einmal, dass die Bankenbranche nicht auf einen Schlag die gesamte IT-Infrastrukturlandschaft verändern und Prozesse beliebig umstellen kann. Allerdings sind die geplanten Maßnahmen im Sinne einer möglichst umfassenden Ist-Analyse des Risikozustands

[533] Vgl. www.telecash.de/telecash/wir_info/international/international.htm
[534] Anderson (2001), S. 205.
[535] Anderson (2001), S. 205 f.
[536] Loscocco (1999) zitiert in Arnfield (2000), S. 18.
[537] Vgl. Arnfield (2000), S. 15 f.

und der Etablierung robuster Risiko-Managementprozeduren, die auf die Problematik Operationeller Risiken zugeschnitten sind, von großer Bedeutung.

Grundsätzlich gibt es wie oben gezeigt bei den branchenunspezifischen Ansätzen für Risikomanagement nur bei der ISO-Norm 17799 Vorgaben und Vorstellungen, in welche Richtung ein adäquater Risikomanagement-Prozess ausgerichtet sein muss, ohne dass die Norm dabei ins Detail geht. Für die Bankenwelt wird jedoch aufgrund der zu erwartenden rechtlichen Rahmenbedingungen der Operational Risk Management-Prozess, den die BIZ vorgibt, das relevante Vorgehen bestimmen. Allerdings wird bei den folgenden Ausführungen deutlich, dass die BIZ sich mit ihren Empfehlungen teils sehr eng an ISO 17799 anlehnt.

5.3.1.2 Anforderungen an das Operational Risk Management nach Basel II

Anderson kommt in seiner Betrachtung über Sicherheitsprobleme im Zahlungsverkehr zur Erkenntnis, dass der Idealzustand die Ergänzung technischer Maßnahmen um organisatorische wäre, unterlegt mit entsprechenden Managementverantwortlichkeiten.[538] In der Folge leitet er einige Schwierigkeiten ab, auf die ein adäquates Risikomanagement reagieren muss, und die sich wie ein roter Faden durch die bekannt gewordenen Fälle Operationeller Risiken ziehen, die zu Schadensfällen geführt haben:[539]

- „It's not always obvious which transactions are security-sensitive.
- It's hard to maintain a working security system in a changing environment.
- If you rely on customer complaints to alert you to fraud, you had better listen to them.
- There will always be people in positions of relative trust who can get away with a scam – for a while.
- No security policy will ever be completely rigid; there will always have to be workarounds for people to cope with real life, and some of these workarounds will create vulnerabilities.
- It's often hard to tell at first sight whether an exception is due to fraud or to error. So the lower the transaction error rate the better."

In Basel II werden diese Probleme bei den Anforderungen an das Operational Risk Management adressiert. Insbesondere werden in dem Paper „Sound Practices for the Management and Supervision of Operational Risk"[540] („Sound Practices") der BIZ organisatorische Maßnahmen im Umgang mit Operationellen Risiken aufgeführt, die im Folgenden dargelegt werden sollen.

In ihrer Analyse der Operationellen Risiken über die letzten fünf Jahre kommt die BIZ zum Schluss, dass diese Art Risiko bei den meisten Banken nur innerhalb von Geschäftsbereichen und im Rahmen interner Audits eine Rolle gespielt hat – wenn überhaupt.[541] Das Entstehen geeigneter Managementansätze, die das gesamte Umfeld der Finanzinstitute mit einbeziehen, ist erst in jüngster Zeit Gegenstand der Betrachtung.[542] Die BIZ versucht, gemeinsam mit den Finanzinstituten einen Ansatz zu definieren, mit dem Operationelle Risiken geeignet adressiert werden können.

[538] Vgl. Anderson (2000), S. 192 f.
[539] Anderson (2000), S. 193.
[540] Vgl. BIZ (2003a).
[541] Vgl. BIZ (2003a), S. 3 Ziffer 8.
[542] Vgl. u.a. Anders (2001), Stocker et al. (2001), Interexa (2002).

Anhand des erweiterten Sicherheitsbegriffs im Schalenmodell, wie in Abbildung 4 dargelegt, wird deutlich, welche neuen Bereiche das Operational Risk Management integrierend abdecken muss, um erfolgreich diese Klasse an Risken zu beherrschen und zu reduzieren. Lag bislang, auch bedingt durch den Einsatz neuartiger Technologien, die Konzentration der Risikoanalyse auf der innersten Schale der IT-Sicherheit, so werden nun vermehrt die äußeren Schalen mit einbezogen. Dies erfordert in den meisten Finanzinstituten eine neue organisatorische Ausrichtung auf die Belange des Operational Risk Managements.

Die Erwartungen der BIZ im Rahmen der Basel II-Arbeiten über Operational Risk Management werden bei den „Sound Practices“ in Form von zehn Grundsätzen dargelegt und vertieft.[543] Im Hinblick auf eine spätere aufsichtliche Überprüfung der bankinternen Strukturen zum Management Operationeller Risiken kann erwartet werden, dass diese Grundsätze die Richtschnur aufsichtlicher Anforderungen darstellen. Die ersten drei Grundsätze beschäftigen sich mit einer geeigneten Umgebung für das Risiko-Management, vier weitere Grundsätze adressieren die eigentliche Identifizierung, Bewertung, das Überwachen und das Beherrschen oder die Kontrolle der Operationellen Risiken. Zwei Grundsätze widmen sich der Rolle der Aufsicht und ein Grundsatz der Rolle der Offenlegung der Bemühungen der Finanzinstitute um ein besseres Operational Risk Management.

Die Bedeutung der einzelnen Grundsätze für das Management Operationeller Risiken und die Konkretisierung durch die Aufsicht wird bei der Darstellung des Risikomanagementprozesses in Abschnitt 5.3.2 herausgearbeitet.

[543] Vgl. BIZ (2003a).

Prinzip	Kurzbeschreibung
Entwicklung einer geeigneten Risiko Management Umgebung	
1	Verantwortung für Operational Risk Management auf Vorstandsebene aufhängen
2	Interne Prüfprozeduren für Überprüfung des Operational Risk Managements und geeignetes Personal notwendig
3	Verantwortung für adäquate organisatorische Umsetzung des Operational Risk Managements liegt bei Führungspersonal
Risiko Management: Identifizierung, Bewertung, Überwachung und Beherrschung/Kontrolle	
4	Maßnahmen zur Identifizierung und Bewertung Operationeller Risiken bei allen Finanzprodukten, Prozessen und Systemen müssen ergriffen werden
5	Überwachung der Entwicklung Operationeller Risiken und Berichtspflicht an Vorstand
6	Implementierung geeigneter Maßnahmen um Operationelle Risiken zu beherrschen und zu kontrollieren
7	Notfallpläne beim Eintritt gravierender Schadensfälle müssen existieren
Die Rolle der Aufsicht	
8	Die Aufsicht sollte für alle Finanzinstitute ein ausreichendes Operational Risk Management fordern
9	Die Aufsicht sollte dieses Management regelmäßig überprüfen und auf aktuelle Entwicklungen reagieren können
Die Rolle der Offenlegung	
10	Die Finanzinstitute sollten ihre Maßnahmen im Bereich Operationeller Risiken so offen legen, dass andere Marktteilnehmer ausreichend informiert sind

Tabelle 8: Die zehn „Sound Practices"-Grundsätze für Operational Risk Management in Finanzinstituten aus Sicht der BIZ im Überblick[544]

5.3.1.3 Bedeutung des elektronischen Zahlungsverkehrs innerhalb der Operationellen Risiken

Innerhalb der Operationellen Risiken stellen die Risiken im Zahlungsverkehr, wie bei der Klassifikation der Risiken deutlich wurde, lediglich einen, allerdings schwierig zu beziffernden, Anteil am Gesamtrisiko. Aus verschiedenen Gründen jedoch ist es gerade im Zahlungsverkehr von besonderer Bedeutung, die Operationellen Risiken zu beherrschen.

Der wohl wichtigste Grund liegt in der Eigenart der Zahlungssysteme und der begrenzten Verfügbarkeit von Bargeld begründet. Bestehen aufgrund hoher öffentlich werdender Risiken im Zahlungsverkehr, sowohl im Groß- als auch im Massenzahlungsverkehr, Ängste oder

[544] Nach BIZ (2003a), S. 4 f, eigene Darstellung.

Misstrauen in der Bevölkerung, kann eine Bank-Run-Automatik losgetreten werden. Diese würde wie oben dargelegt den Bestand des Bankensystems gefährden.

Elektronischer Zahlungsverkehr wird im täglichen Leben nur bei Störfällen wahrgenommen. Diese Wahrnehmung ist schnell eine kritische Größe, die ein besonderes Augenmerk auf die Sicherheit des elektronischen Zahlungsverkehrs rechtfertigt. Wer einmal den Effekt erlebt hat, den eine Durchsage in einem bekannten schwedischen Möbel- und Einrichtungshaus zur besten Samstag-Einkaufszeit bewirkt, die verkündet, elektronische Zahlungen wären auf unbestimmte Zeit wegen technischen Problemen weder mit EC-Karte noch mit Kundenkarte möglich, der weiß, was mit dieser Aussage gemeint ist.[545] Ebenso eindrucksvoll das kollektive Aufatmen als per Durchsage ungefähr 30 Minuten später der Fehler für behoben erklärt wurde – und die Besitzer wieder zu ihren verwaisten Einkaufswagen zurückkehrten.

Die zunehmende Elektronisierung weiter Bereiche der Gesellschaft im Allgemeinen und des Zahlungsverkehrs im Besonderen[546] ist in wesentlichen Teilen von dem Vertrauen der Bevölkerung in die technischen Systeme abhängig. Für den Zahlungsverkehr und die besondere Aufgabe der Aufsicht hat dies Santormero, Präsident der Philadelphia Federal Reserve Bank, so formuliert: „Payments in any form, at any time, reflect the degree of trust market participants place in the institutions governing them.“[547] Gibt es keinen eTrust[548] oder zu viele Ereignisse jedweder Art, die diesen eTrust erschüttern, wird das Tempo der Elektronisierung verlangsamt und im Extremfall der Prozess gefährdet.

Eine Umfrage unter europäischen Konsumenten, in Auftrag gegeben von der EU-Kommission zeigt eine große Länder-Diskrepanz bei der wahrgenommenen Sicherheit gegenüber elektronischen Zahlungsverkehrsinstrumenten. Bei einem Maximalwert von 10 wurden für den so genannten Vertrauensindikator in Griechenland 5,25 erreicht, Deutschland lag mit 7,34 im Mittelfeld, Finnland führte mit 8,41.[549] Insbesondere bestehen aus Sicht der Konsumenten große Ängste in den Bereichen Sicherheit, Betrug und Schutz der Privatsphäre.

Ein weiteres Argument für eine erhöhte Bedeutung des Zahlungsverkehrs bei Operationellen Risiken findet sich im Eingangszitat. Zahlungsverkehr und seine Manipulation, im Extremfall die perfekte Fälschung elektronischen Geldes als Duplikat, ermöglichen ohne Umwege direkte monetäre Vorteile bei kriminellen Taten – Anreiz genug, zumindest auf mittlere Sicht.

Die absolute Bedeutung von Vorfällen, bei denen Ereignisse aus dem Umfeld Operationeller Risiken zu tatsächlichen oder Beinahe-Schadensfällen geführt haben, lässt sich sehr schwer einschätzen. Im optimistischen Fall kann aus der geringen Dichte an Veröffentlichungen zum Thema Schadensfälle im elektronischen Zahlungsverkehr deren Bedeutungslosigkeit abgeleitet werden. Im schlechtesten Fall sind die Berichte über Schadensfälle nur die Spitze des Eisbergs und die betroffenen Banken und Dienstleister versuchen wegen der schlechten Außenwirkung alles, um eine Lösung zu finden, die in keine Statistik Einzug hält und zukünftigen Schaden (und auch Nachahmer) verhindert.[550] In diese Richtung argumentiert Schneier, der feststellt[551]: „When a DC-10 falls out of the sky, everyone knows it. [...] Security debacles are different; there’s often no fireball and no immediate repercussions. Most

[545] Eigenes Erlebnis des Autors im Herbst 2001.
[546] Vgl. EZB (2003a).
[547] Santomero, A. M. in: Sienkiewicz und Bochicchio (2002), S. 3.
[548] Vgl. HVB (2001).
[549] EU (2003)., S. 2.
[550] Vgl. BSI (2000), S. 1.
[551] Schneier (2000), S. 191.

successful attacks – against banks, against corporations, against governments – go unmentioned in the media. Some of them even go unnoticed by the victims." Auch Thodén argumentiert nach den von ihr geführten Experteninterviews:[552] „Many of the experts in banks and insurance companies interviewed believe that there is a lot more IT related crime in the banking industry than what is public knowledge."

Neben schlechter Presse für ein betroffenes Unternehmen wird durch das Einschalten der Polizei deren Ermittlungsapparat innerhalb des Unternehmens in Gang gesetzt.[553] Power geht noch einen Schritt weiter und vermutet, dass bereits die Tatsache, dass ein Unternehmen keine Schadensfälle mitteilt oder keine Ereignisse in der Presse präsentiert werden, in der Außensicht ein Pluspunkt ist, beziehungsweise angenommen werde, es gäbe auch keine Vorkommnisse in ebendiesem Unternehmen.[554] Ein Vorfall bei der Citibank aus dem Jahr 1995 gibt den Anhängern zögernder Öffentlichkeitsarbeit im Hinblick auf Schadensfälle recht.[555] Citibank verlor durch einen russischen Hacker USD 12 Mio. Die Citibank nutzte dieses Ereignis, um umfangreiche neue Sicherheitsmaßnahmen zu ergreifen und der Öffentlichkeit mitzuteilen, solche Vorfälle gehörten nunmehr der Vergangenheit an. In der Folge jedoch, so Schneier, zogen besorgte Kunden Millionen von US-Dollars von der Bank ab, weil sie befürchteten, ihr Geld wäre bei der Citibank unsicherer als bei anderen Banken. Die „lesson learnt" der Citibank lässt sich im Licht dieser Ereignisse verstehen: „Don't publicize."

Von einem anderen bemerkenswerten Grund für das Nicht-Melden eines Schadensereignisses berichtet Thodén im Rahmen eines Experteninterviews.[556] Demzufolge hatte eine japanische Bank in London einen Schadensfall im höheren zweistelligen Millionen Pfund Bereich. Allerdings verzichtete die Bank auf die Inanspruchnahme einer vorhandenen Versicherungspolice – aus Angst, die Versicherung könnte ihre Computersysteme in der Folge dieses Vorfalls genauer unter die Lupe nehmen.

Die Wahrheit in Bezug auf Statistiken über Zahlungsverkehrsbetrug wird zwischen der optimistischsten und pessimistischsten Annahme angesiedelt sein.

Eines ist zumindest bisher so gut wie sicher und wird von technischen Experten wie Ross Anderson bestätigt: In den seltensten Fällen, in denen Schaden verursacht wird, ist das Überwinden komplexer technischer Hürden die Ursache für einen Erfolg. Meist sind erfolgreiche Angriffe eher über Umwege, die ebendiese Hürden außer Kraft setzen, realisiert worden. So ist beispielsweise das Nachrichtendienstsystem SWIFT für Großzahlungen in 20 Jahren nicht einmal von Außen erfolgreich angegriffen worden.[557]

Generell werden Finanzinstitutionen neben High-Tech-Unternehmen bei Analysen, die branchenspezifische Unterschiede herausarbeiten, am häufigsten über das Internet angegriffen.[558] Für die USA gilt dabei, dass Angriffe auf die Finanzindustrie in besonderem Maße vom asiatischen Raum ausgehen. Die Angriffsrate liegt 55-70 % höher als beim Durchschnitt aller Industrien. Ein interessantes Detail liefert die Untersuchung der eCommerce-Unternehmen. Diese werden entgegen den Erwartungen signifikant unterm Gesamtdurchschnitt im Netz angegriffen.

[552] Thodén (1999), S. 97.
[553] Vgl. Power (2002), S. 14 f.
[554] Vgl. Power (2002), S. 15.
[555] Vgl. Schneier, S. 391 f.
[556] Vgl. Thodén (1999), S. 67 FN 48.
[557] Anderson (2001), S. 194 ff.
[558] Vgl. Belcher (2002), S. 19 ff.

Schadensfälle durch Operationelle Risiken entstehen wie bereits in der Definition ausgeführt nicht ausschließlich durch Angreifer, seien es Innen- oder Außentäter, Einzeltäter oder kriminelle Gruppierungen. Gleichwohl stellt das bewusste Ausnutzen von Systemschwächen, technischen wie organisatorischen, eine besondere Gefahr da. Dies gilt in finanzieller Hinsicht, gerade wenn Wiederholungsmöglichkeiten bestehen, aber auch in Hinblick auf die öffentliche Wirkung. Bei kriminellen Taten droht automatisch ein zusätzlicher Publizitätseffekt, verstärkt durch polizeiliche Ermittlungen und mögliche öffentliche Gerichtsverfahren.

Einen ersten Eindruck über die tatsächliche Bedeutung von externen und internen Angriffen gibt die vom Baseler Ausschuss für Bankenaufsicht durchgeführte Quantitative Impact Study 3 (QIS3), bei der auch die Erfassung Operationeller Risiken eine wesentliche Rolle spielte. Entgegen anderslautenden Berichten, die internen Betrug zu einem der häufigsten Schadensfälle im kriminellen Bereich stilisieren[559], kommt die Auswertung bei 89 Banken zu einem gänzlich anderen Ergebnis. Zwar stellt Betrug insgesamt die höchste einzelne Schadenskategorie, allerdings sind es Angriffe von Außentätern, die zu 43,94 % für Schäden verantwortlich sind. Internen Tätern können lediglich 3,50% der Fälle zugerechnet werden; es sei darauf aufmerksam gemacht, dass dies nicht bedeutet, dass nur in dieser Größenordnung interne Betrugsfälle auftreten; hier handelt es sich um die entdeckten und im Rahmen der Studie gemeldeten Fälle. Der nächste große Block sind mit 35,40 % Fehler bei der Prozessverarbeitung (ohne kriminellen Hintergrund).[560]

Für andere Schäden, die durch Operationelle Risiken entstehen, fehlen in noch stärkerem Maße verfügbare Statistiken. Die Möglichkeiten für betroffene Institutionen, diese Ereignisse „im Haus“ zu halten, sind zudem dann ungleich größer, wenn „nur“ interne Prozesse betroffen sind. In Fällen, in denen offensichtliche fehlerhafte Prozeduren auch mit Außenwirkung verbunden sind, beispielsweise bei von Unbefugten einzusehenden Kontodaten Dritter im Internet nach einem fehlerhaften Software-Update, ist Pressewirkung meist ebenso garantiert wie bei kriminellen Taten. Im Rahmen der QIS3 konzentrieren sich bei den teilnehmenden Banken die Risiken offensichtlich im Bereich „Retail Banking“. Dort treten 61,10 % aller Schadensfälle auf. Bei acht Geschäftsbereichen und sieben Schadenskategorien lassen sich insgesamt 56 Kategorien betrachten; in 42 der 56 Kategorien konzentrieren sich unter 1 % der Ereignisse bezogen auf die Summe der Schadensfälle.[561]

Die Größenordnungen sind dabei offensichtlich, fraglich ist, ob die deutlich unterrepräsentierten Kategorien tatsächlich von so geringer Bedeutung sind, oder ob sich dort in besonderem Maße die Schadensfälle häufen, die durch äußerst geringe Wahrscheinlichkeiten aber hohe Schadenssummen gekennzeichnet sind;[562] bei QIS3 sind unter 2 % der gesamten Schadensfälle solche mit über 1 Mio. Euro Schadenssumme[563] – bei QIS2 waren es noch 1 %[564]. Diese „low frequency, high impact“-Schadensfälle sind in der Betrachtung der Gesamtschadenshöhe allerdings von erheblicher Bedeutung. In QIS2 machten diese Schäden wertmäßig drei Viertel aus, in QIS3 ist diese Relation ähnlich. 2,7 % der Ereignisse sind für 75,7 % der Schadens-

[559] Vgl. Thodén (1999), S. 62 f. Thodén berichtet, dass sowohl die von ihr interviewten Experten von hohen Insiderquoten bei Angriffen ausgehen als auch andere Studien bis zu zwei Drittel der Schadensfälle Angestellten zurechnen.
[560] Vgl. BIZ (2003f), S. 11, Tabelle 7.
[561] Vgl. BIZ (2003f), S. 6 f.
[562] Vgl. BIZ (2003f), S. 40.
[563] BIZ (2003f), S. 2.
[564] BIZ (2002a), S. 9.

summe zu ermitteln, lediglich 0,2 % der Schadensereignisse vereinen 48,3 % der Schäden auf sich.[565]

Eine andere Möglichkeit besteht darin, dass die Mitarbeiter in den anderen Bereichen noch keine Wahrnehmung für bestimmte Schadensfälle entwickelt haben und das Erheben der Schadensfälle dadurch (noch) problematisch ist. In diesem Fall kann der relativ kurze Betrachtungszeitraum in Kombination mit einer verhältnismäßig geringen Anzahl teilnehmender Banken und vorhandenen Erhebungsproblemen bei den Banken zu einem falschen Sicherheitsgefühl in diesen Bereichen fühlen. Im Retail-Banking Bereich hingegen finden sich bei Betrachtung der Schadenssummen überproportional viele Schadensfälle mit höheren Eintrittswahrscheinlichkeiten aber geringerer Schadenssumme. Trotz über 60 % Anteil an den Schadensfällen zeichnet dieser Bereich „nur" für 29 % der Schadenssumme verantwortlich, bleibt damit allerdings in Relation zu den anderen Geschäftsbereichen immer noch an erster Stelle.[566] Auffällig ist die Relation beim Commercial Banking. Mit einem Anteil von 7 % der Schadensfälle wird eine Größenordnung von 29 % der Schadenssumme erreicht.[567]

Die Datenerhebung und dynamische Entwicklung im Bereich Operational Risk Management erschwert Vergleiche zwischen einzelnen Erhebungen. Die Verteilung der Schadensfälle auf die Geschäftsbereiche ist von 1998 – 2001 ähnlich zu 2002. Auch in der für die Jahre 1998 bis 2001 durchgeführten Analyse zeichnete der Bereich Retail-Banking für 67,43 % der Schadensfälle verantwortlich, bei einem Schadenswert von 39,41 %.[568] An zweiter Stelle lag Commercial Banking mit 13,21 % der Schadensfälle aber wertmäßigen 22,91 %.

Generell gibt es zum gegenwärtigen Zeitpunkt auf Seiten des Baseler Ausschusses für Bankenaufsicht weiterhin Zweifel an der Qualität des Datenmaterials. Trotz ausführlichen Berechnungen warnt der Ausschuss vor zu weitgehenden Interpretationen der empirischen Befunde[569]: „It is also not clear the extent to which the sample of banks in the survey was representative of the banking industry as a whole." Eine analoge Aussage findet sich auch zu den QIS2 Daten von 1998 – 2001.[570]

5.3.1.4 Unterschiedliche Anforderungen an das Risiko-Management bei Massen- und Großbetragzahlungssystemen

Sowohl Großzahlungssysteme als auch Massenzahlungssysteme arbeiten mittlerweile in offenen Netzen. Gleichwohl unterscheiden sich die einzelnen Verfahren unter anderem in Bezug auf die Anzahl der Teilnehmer, die Zugangsvoraussetzungen zum jeweiligen System und die Höhe der verarbeiteten Beträge, wie in Kapitel 4 deutlich geworden ist, erhelblich.

Der größte Unterschied liegt in der möglichen Anzahl beteiligter Personen oder Institutionen an einem Bezahlvorgang. Während bei den Großzahlungssystemen die Anzahl der Akteure stark eingeschränkt ist und klare sicherheitsrelevante Zugangsbarrieren existieren, zeichnen sich die Retail-Bezahlverfahren durch den potenziellen Zugang praktisch aller in einer Volkswirtschaft beteiligten Akteure aus.

Die Größenordnungen des Großzahlungssystems liegen über denen des Massenzahlungsverkehrs, die Anzahl der Transaktionen ist signifikant geringer. In der Folge lassen sich a)

[565] BIZ (2002a), S. 9, BIZ (2003f), S. 10.
[566] Vgl. BIZ (2003f), S. 8.
[567] BIZ (2003f), S. 6 f.
[568] BIZ (2002a), S. 8 f.
[569] BIZ (2003f), S. 16.
[570] Vgl. BIZ (2002a), S. 6.

leichter Kontrollen und Sicherheitsmechanismen rechtfertigen und b) ist die Aufsicht an den system-kritischen Zahlungssystemen im Großbetragsbereich besonders interessiert.

Für die Großzahlungssysteme kann mittlerweile eine Tradition der Sicherheitskonzeption festgestellt werden. Mehrere Systemwechsel, die Integration neuer Verfahren wie RTGS^{plus} und kritische Phasen wie die Jahr-2000-Umstellung und der Terroranschlag des 11.09.2001 wurden erfolgreich überwunden. Die Transaktionszahlen und –volumina der Systeme steigen stetig und seit Jahren, ohne nennenswerte Publikationen über Schadensfälle.

Ein anderes Bild zeichnet sich bei den Retail-Bezahlverfahren in offenen Netzen ab. Deren Entwicklung steht – bis auf den Einsatz der Kreditkarte (bei entsprechenden Sicherheitsproblemen und negativer Publicity) – zumeist am Anfang. Die Transaktionszahlen sind meist gering, die Volumina unbedeutend. Gleichwohl ist der Aufsicht bewusst, dass dieser Zustand sich zunehmend ändern wird. Der eCommerce verzeichnet hohe Zuwachsraten, Bezahlvorgänge werden immer öfter elektronisch abgewickelt. Damit steigt das Risiko fehlerhafter Prozesse und betrügerischer Manipulation, die französische Zentralbank beginnt an die Betreiber der Systeme strengere Anforderungen zu stellen und auch die Deutsche Bundesbank und die EZB formulieren zunehmend Sicherheitsziele und appelieren an die Selbstregulierung des Marktes.[571]

Grundsätzlich werden die Großzahlungssysteme von Banken und Dienstleistern, die im Besitz und unter Aufsicht der Banken sind, betrieben. Die Massenzahlungssysteme sind ebenso unter Bankenkontrolle. Mit zunehmenden Ausnahmen und Kooperationen verschiedener Akteure könnte der Zugang zu diesem Markt eventuell aber auch Dritten möglich werden, dem KWG folgend zwar unter Kontrolle oder Auftragsvergabe einer Bank aber in der Durchführung zunächst selbständig tätig. Hinzu kommen zusätzlich europäische Dienstleister, die eine lokale Zulassung der Aufsicht erhalten und gemäß EU-Recht auch in Deutschland tätig werden könnten – bislang ist dieser Fall nur bei Moneybookers eingetreten, einem eMail-basierten Bezahldienst, der nicht im Besitz von Banken ist und von der britischen Aufsicht die erste Banklizenz gemäß EU-Richtlinie 2000/46/EG erhalten hat.

Für alle Systeme ist eine zunehmende Abhängigkeit der Banken und Zahlungssystem-Abwickler von dritten IT-Dienstleistern festzustellen. Einerseits bedingt durch die technologische Entwicklung, andererseits durch Outsourcing-Bemühungen, beispielsweise bei dem in der Branche bislang größten Outsourcing-Vertrag zwischen Deutscher Bank und IBM. Der Auftrag vergibt wesentliche Teile der Dienstleistung im Bereich IT-Infrastrukur der Deutschen Bank für mindestens 10 Jahre an IBM.

Neben den aufsichtlichen Vorgaben wird eine Unterscheidung auch aus (haftungs)rechtlichen Überlegungen heraus notwendig. Bei den Großzahlungen sind die Bestimmungen aufgrund der Höhe der Beträge eindeutig, Streitfälle gibt es aufgrund des vertraglich gestalteten Rahmens praktisch nicht. Die Einhaltung der Lamfalussy-Kriterien hat Wirkung gezeigt.

Anders bei Massenzahlungen, bei denen eine Vielzahl Akteure (u.a. Händler, Kunden, Banken, Dienstleister) in den Bezahlvorgang involviert sind, und somit insbesondere haftungsrechtliche Fragen im Schadensfall unsicher werden. Gerade bei den innovativen Bezahlverfahren sollte die rechtliche Konstruktion untersucht werden, unter anderem um die Haftungsobergrenzen der Betreiber zu kennen. Diese Obergrenzen ermöglichen dem Betreiber eine erste Abwägung des Aufwands für die notwendige Sicherheit. Die offensichtli-

[571] Vgl. für die Entwicklung in Frankreich Beau (2002), für die EZB EZB (2003b) und für die Deutsche Bundesbank Fabritius (2003a).

che Gefahr besteht darin, dass ein mittelständischer Betreiber, sollte sein System korrumpiert werden, unter Umständen nicht in der Lage ist, seinen Verpflichtungen nachzukommen.

Bei den Einzelsystemen im Massenzahlungsverkehr kann eine Abschätzung klären, ob die Systeme vor allem von der aufsichtlichen Seite mit Sicherheitsanforderungen konfrontiert werden, oder vermehrt von der betriebswirtschaftlichen Seite bei zunehmendem Einsatz der Systeme effiziente Sicherheitsmaßnahmen erforderlich werden.

Bei den Großzahlungssystemen ergeben sich im Rahmen der Euro-Einführung vermehrt Möglichkeiten „economies of scale“ auszunutzen. In der Folge dominieren wenige Einzelsysteme – in Europa an der Spitze das System RTGS^{plus} der Deutschen Bundesbank – den Markt, mit in der Folge sinkender Komplexität der wechselseitigen Beziehungen. Dies führt zu einem Mehr an Sicherheit, da die Kontrollmechanismen einfacher zu implementieren und zu überprüfen sind. Die klare Tendenz zu Real-Time Clearing und Settlement minimiert das Risiko unentdeckter krimineller Manipulationen und von unbeabsichtigten Transaktionsfehlern zusätzlich.

Im Licht der bekannt gewordenen Schadensfälle, die (bisher) nicht auf technischen Angriffen basieren, sondern auf dem Ausnützen organisatorischer Schwachstellen, scheint eine bessere Kontrollstruktur in diesem Bereich von Bedeutung. Dabei geht es zum einen darum, die alternativen Übertragungswege von Großzahlungen, die an den technisch gesicherten Netzen vorbeigehen, wie z. B. Anweisungen mittels beglaubigtem Telex, besser in die Kontrollstrukturen einzubinden. Zum anderen kann aus der Erfahrung in diesem Bereich – in die meisten bekannt gewordenen Angriffe sind Innentäter involviert – geschlossen werden, dass notwendige und etablierte Kontrollstrukturen weitgehend intransparent in Bezug auf die gesamte Prozesskette bleiben oder werden sollten. Damit wird die Unsicherheit für potenzielle Angreifer und die Wahrscheinlichkeit ihrer Entdeckung stark erhöht. Die geforderte Intransparenz gilt jedoch nicht für die technologische Infrastruktur, insbesondere nicht beim Einsatz kryptographischer Verfahren. Dort hat sich der Gedanke der Transparenz durchgesetzt. Hintergrund ist, dass die Stärke eines kryptographischen Verfahrens nur durch internationale Experten und vielfache Angriffsversuche und Untersuchungen aus verschiedenen Blickwinkeln bestätigt werden kann. Eigenentwicklungen, die auf dem „security by obscurity“-Ansatz beruhen, sind äußerst fehleranfällig und meist leicht zu überwinden. Musterbeispiele für gescheiterte Eigenentwicklungen liefern die Verfahren, die zunächst bei Decodern im Pay-TV eingesetzt wurden aber auch der aus Sicht seiner Erfinder vermeintlich sichere DVD-Kopierschutz.

Unterschiedlich stellt sich die Situation bei den Massenszahlungssystemen dar. Die Entwicklung der letzten Jahre lässt nicht erkennen, dass es in Kürze zu einer Konvergenz bestehender Systeme kommen wird. Dies gilt in besonderem Maße für die Zugangsprodukte zu den Banknetzen. Dort werden verstärkt Sicherheitsanstrengungen der Akteure notwendig werden, um die Kompromittierung der anschließenden Systeme durch das Einschleusen manipulierter Transaktionen zu verhindern.

Im Gegensatz zu den Großzahlungssystemen, bei denen eine lang erprobte Sicherheitskultur im Kreis ausgewählter Akteure vorherrscht, sind die Akteure im Massenzahlungsverkehr deutlich heterogener. Ein Ende dieser Entwicklung ist nach den Erkenntnissen aus der Betrachtung der strategischen Rolle der verschiedenen Akteure (siehe Abschnitt 4.2.6.5) nicht absehbar. Vielmehr werden beispielsweise im Bereich der Telekommunikationsunternehmen neue Bezahlverfahren erprobt, die Kreditkartengesellschaften setzen neuartige Technologien Dritter ein und die ersten Nicht-Banken überlegen auch in Deutschland den Erwerb einer

Banklizenz, um die Finanzinstitute auf ihrem ureigenen Terrain der Transaktionsabwicklung anzugreifen.

Diese Heterogenität bringt für die prozesshafte Betrachtung der Sicherheit eigene Probleme mit sich, die auch aufsichtliche Belange und Prüfmechanismen einschließen. Die offenen Fragen liegen im Bereich der Abnahme der Sicherheitsvorkehrungen bei outgesourcten Dienstleistern, bei Dienstleistern, die im Bereich der Datenverarbeitung ausserhalb des direkten Zugriffs der Bankenaufsicht agieren und bei Fragen der Messbarkeit von Sicherheitsvorgaben.

5.3.2 Operational Risk Management: die Prozessschritte

Zunächst gilt es, die Risiken zu identifizieren, anschließend muss eine Quantifizierung und Bewertung dieser Risiken erfolgen. Erst auf dieser Grundlage können die Steuerungsinstrumente eingesetzt werden, die das Management Operationeller Risiken ermöglichen. Abschließend kann der gesamte Prozess des Risikomanagements der Kontrolle interner und externer Prüfer unterzogen werden. Der Prozess selbst ist dynamisch, Änderungen können fortlaufend eingepflegt werden.

5.3.2.1 Identifikation

Die Identifikation der Operationellen Risiken, ihre Bewertung und Quantifizierung stellen die Grundlage des Risikomanagements dieser Risiken dar.

In einem sensiblen Geschäftsfeld wie dem Zahlungsverkehr gilt der für die externe Erfassung von Schadensfällen plakative Ausspruch von Jameson in besonderem Maße:[572]
„The figures available are probably comparable to a door-to-door survey on the number of crazy people in society. Would you tell them about Uncle Johnny unless he was hanging out of the dow?"

In den nächsten beiden Abschnitten finden sich daher zunächst ausgewählte und bekannt gewordene Schadensfälle durch Operationelle Risiken im Retail-Zahlungsverkehr und bei Großzahlungen. Anschließend werden die Anforderungen, die durch Basel II an die Identifizierung dieser Risiken gestellt werden, dargelegt.

5.3.2.1.1 Operationelle Risiken und ausgewählte Schadensfälle im Retail-Zahlungsverkehr

Es gibt einige öffentlich gewordene Fälle, die geradezu Mustervorlagen für das Vorkommen und Ausnutzen Operationeller Risiken darstellen. Im folgenden werden auf dem Gebiet des elektronischen Zahlungsverkehrs einige Beispiele genannt. Insbesondere an den Stellen, an denen auf Zeitungsberichte verwiesen wird, ist naturgemäß Vorsicht bei der Interpretation der Details geboten.[573] So kommen unterschiedliche Autoren gelegentlich bei der Darstellung eines Ereignisses zu unterschiedlichen Fakten. Oft ist allerdings auch weniger die absolute Schadenshöhe von Bedeutung, sondern vielmehr das Aufzeigen einer Schwachstelle und der Tatsache, dass diese ausgenutzt wurde. Grundsätzlich sollen auch die aufgeführten Fälle potenzielle Operationelle Risiken und ihre Bedeutung aufzeigen, gleichwohl im Bereich der Groß- wie der Massenzahlungen.

[572] Jameson (1998), zitiert in Beeck (2000), S. 652.
[573] Darauf verweist explizit Thodén (1999), S. 66 FN 46. Selbst bei den von ihr geführten Experteninterviews ist selten ein Schadensfall aus erster Hand, vielmehr nur vom Hörensagen bekannt.

Gemäß dem Schneierschen Diktum des Eingangszitat zu Abschnitt 5.3, demzufolge Angriffe dort stattfinden, wo Geld vermutet wird, sind Geldausgabeautomaten ein natürliches Ziel von Angreifern. Ein Schutzmechanismus für Automaten ist der Einsatz kryptographischer Verfahren in der Kommunikation der Automaten im Netzwerk. Da bei symmetrischen Schlüsseln zu viele Schlüssel jedem bekannt sein müssten, gibt es Schaltstellen, die über die notwendigen Schlüssel verfügen, und über die die Geldausgabeautomaten mit dem Netzwerk, beispielsweise VISA, kommunizieren. Anderson berichtet von einem Fall, in dem die Verschlüsselungskomponenten in einer solchen Schaltstelle durch einen Innentäter (Manager der Schaltstelle) ausgehebelt wurden. Der verursachte Schaden ging in die Millionen GBP.[574]Im Retail-Zahlungsverkehr sind Angriffe auf Geldautomaten vermutlich die häufigste Schadensquelle. Die Sachlage bei Angriffen auf Geldausgabeautomaten stellt sich (immer noch) kritisch dar. Seit der Installation der ersten Automaten Ende der sechziger Jahre werden sie immer wieder mit Erfolg angegriffen. Anderson spricht in diesem Zusammenhang von „epidemics of fraud from ATMs“[575],[576] und verweist auf die jüngste erfolgreiche Angriffswelle Ende 2002, Anfang 2003. Operationelle Risiken spielen bei diesen Fällen eine wichtige Rolle und die Versuche der betroffenen Banken, die Informationen über die Schwachstellen der Systeme und einzelner Baureihen von Geldausgabeautomaten geheim zu halten, zeigen, dass sich der Umgang mit diesen Risiken auch nach 30 Jahren Erfahrungen mit Angriffen schwierig gestaltet. Der Gerichtsfall, in dem Ross Anderson nunmehr als Experte für Computer-Sicherheitstechnik die Angeklagten vertritt, zeigt exemplarisch die potenzielle Sprengkraft von Angriffen auf Massenzahlungssysteme und ihre Netzwerke.[577]

Mike Bond und Piotr Zielinski weisen in einem Technical Report der Universität von Cambridge nach, dass es weitaus einfacher als bisher angenommen ist, die PIN[578] aus einem hardwarebasierten Sicherheitsmodul auszulesen; mit drastischen Folgen für potenzielle Innen- wie Außentäter und die resultierenden Schadenssummen.[579] Bond und Zielinski beweisen Mithilfe der Technik adaptiver Dezimalisation und geschicktem Erraten, die Möglichkeit, in durchschnittlich 15 Versuchen eine vierstellige PIN zu ermitteln; für die Risikoberechnungen wurde bislang von 5.000 notwendigen Versuchen ausgegangen. Die Technik kann bei verschiedensten Geldausgabeautomaten angewendet werden, da sie auf einer Schwachstelle der hardwarebasierten Sicherheitsmodule basiert, die im Geldausgabeautomaten die PIN-Überprüfung übernehmen. Diese Module finden sich bereits in Geldausgabeautomaten der achtziger Jahre; die zugrundeliegenden Methoden wurden nicht weiter modifiziert. Ein möglicher Angriff geht von einem Mittäter in der Bank aus, der beispielsweise mit der neuen Technik in einer Mittagspause von 30 Minuten statt bisher 24 PINs ungefähr 7.000 Nummern erraten kann. Der potenzielle Schaden, den ein Täter in der Bank mit der Weitergabe der PIN an Dritte, die dieses Wissen ausnutzen, anrichten kann, steigt dabei von GBP 7.000 auf GBP 2,1 Mio. Ein einzelner Angreifer, so Bond und Zielinski, könnte an einem Tag durch Abheben am Automaten einen Schaden in Höhe von GBP 30.000 bis 50.000 anrichten. Damit werden aus tolerierbaren Sicherheitslücken mit überschaubaren Schadenssummen im Zweifel existentielle Schäden.

Eine weitere Gefahr stellt für die Bankenwelt der Verlust der Verlässlichkeit ihrer eigenen Sicherheitseinrichtungen in der Außensicht dar. Gesetzt den Fall, es kommt zu Schadensfällen

[574] Anderson (2001), S. 199.
[575] Automatic Teller Machine
[576] Anderson (2003), S. 2.
[577] Vgl. Anderson (2003).
[578] Personal Identification Number, ohne die mit Kreditkarten am ATM kein Geld abgehoben werden kann.
[579] Vgl. Bond (2003).

wie im Prozess Diners Club versus Anil und Vanita Singh[580], dann haben die geschädigten Banken unter Umständen massive Probleme das Gericht von der Effektivität ihrer Schutzmaßnahmen zu überzeugen. In diesem Fall klagte Diners Club gegen das Ehepaar Singh, da im März 2000 an einem einzigen Wochenende mit ihrer Diners Club Karte und PIN an 190 Automaten in Großbritannien insgesamt GBP 50.000 abgehoben worden waren; allerdings war das Ehepaar Singh zu diesem Zeitpunkt in Südafrika. Die Anklage geht von Mittätern im Auftrag des Ehepaar Singh aus. Angesichts der wissenschaftlichen Arbeiten in diesem Bereich wird es für die Kläger sehr schwierig, mögliche Restzweifel, es gäbe auch noch andere potenzielle Täter, da die Sicherheitsvorkehrungen relativ leicht zu überwinden wären, zu beseitigen: der Ausgang des Verfahrens im Sinne der Angeklagten wäre kaum zu vermeiden. Anderson kommt auch bei Analyse weiterer Sicherheitsschwachstellen bei ATMs zur Bestätigung der These, dass Banken im Missbrauchsfall erhebliche Beweisprobleme vor Gericht hätten.[581] Ein anderes Problem stellt die öffentliche Verhandlung dar: geschädigte Banken haben kein Interesse, ihre Schutzvorkehrungen bis ins Detail vor Gericht auszubreiten. Im Fall Diners Club versus Singh wurde sogar versucht, die wissenschaftliche Arbeit von Bond und Zielinski, die das schnelle Erraten von PINs darstellt und die Grundlage einer geplanten Doktorarbeit ist, zu vertraulicher Information zu erklären, die nicht veröffentlicht werden dürfe.[582] Die Praxis, sicherheitsrelevante Informationen nur bankinternen Spezialisten zur Verfügung zu stellen, wird auch bei dem vom ECBS herausgegebenen Technischen Report TR407 V1 „Risk of fraudulent PIN capture“ deutlich, der nur für den internen Gebrauch freigegeben ist. Einerseits wird damit erreicht, dass sensible Informationen nicht in falsche (zumindest externe) Hände geraten, andererseits wird verhindert, dass Lücken von der interessierten Fachwelt aufgezeigt werden, bevor sie von kriminellen Innen- oder Außentätern ausgenutzt werden können.

Bond und Zielinski führen weiter aus, dass trotz mehr als 20-jähriger Erfahrung mit hardwarebasierten Sicherheitsmodulen in Geldausgabeautomaten die formale Sicherheitskonzeption noch immer in den Kinderschuhen steckt.[583] Obwohl die Schwachstelle nunmehr bekannt wurde, ist aufgrund der technischen und organisatorischen Ausgestaltung kein einfacher Weg vorhanden, um dieses Risiko in Zukunft zu vermeiden. Lediglich eine bessere Überwachung der PIN-Eingabe und eine Überprüfung der Ursachen bei Fehlversuchen würde als Sofortmaßnahme sicherheitserhöhend wirken können. In ihrer Analyse kommen die beiden Autoren zum Schluss, dass selbst eine teure Neuentwicklung des entsprechenden Moduls keineswegs selbstverständlich eine höhere Sicherheit bietet. Die Schwierigkeit liegt bereits bei der formal korrekten Spezifikation der Sicherheitsziele des entsprechenden Moduls. Fehlende Angriffe in der Vergangenheit haben keinen oder nicht genügend Druck von außen auf die Beteiligten aufgebaut, der die Weiterentwicklung neuer Methoden und Module gefördert oder erzwungen hätte.

Dies ist kein Einzelfall. In Frankreich wurde im Jahr 2000 der Verschlüsselungsalgorithmus der Carte Bleu, einer weitverbreiteten Debitkarte, geknackt. Aufgrund fehlender Maßnahmen für diesen Fall, blieb der Kartenindustrie nur übrig, mit dem Schaden zu leben, oder die gesamten Karten in Frankreich nicht nur zurückzurufen, sondern sofort zu sperren.[584] Schneier nennt einen weiteren Schaden in Kanada, in dem eine Geldkarte die gleichen

[580] Vgl. Anderson (2003).
[581] Vgl. Anderson (2001), S. 199 f.
[582] Vgl. Anderson (2001). In Handelsblatt (2002) wird die Sorge von Banken vor schlechter Publicity und hohen Sicherheitszusatzkosten als Grund für mangelnde Informationen über Sicherheitsprobleme genannt.
[583] Bond (2003), S. 13
[584] Vgl. Schneier (2000), S. 380.

Schwierigkeiten hatte.[585] Er kommt zu dem Schluss, dass bei der Konzeption technischer System nicht nur auf die potenziellen Angriffe und Bedrohungen geschaut werden sollte, sondern auch Maßnahmen geplant werden müssten, die im – unter Umständen auch unwahrscheinlichen – worst case' eines kompromittierten Systems dieses lauffähig halten können.

Dabei wird ein weiterer Aspekt deutlich: Wird das mathematische Verfahren geknackt, auf dem momentan alle kryptographischen Verfahren mit asymetrischer Verschlüsselung beruhen, könnte praktisch kein Geschäftsverkehr und Zahlungsverkehr im Netz mehr ohne das Risiko kompromittiert zu werden, abgewickelt werden. Eine Lösung bieten flexible kryptographische Bausteine wie sie im Rahmen des vom Bundesministerium für Wirtschaft und Arbeit geförderten Projekts FairPay mit der FlexiPKI entwickelt wurden.[586]

Weitere Probleme mit Geldausgabeautomaten, die ihre Ursachen vollständig im Bereich der Operationellen Risiken haben, sind einfache Datenverarbeitungsfehler in den Systemen. Anderson schätzt die Fehlerrate existierender Systeme auf 1 zu 10.000 bis 1 zu 100.000 und geht bei 5 Milliarden ATM-Transaktionen pro Jahr in den USA von bis zu 50.000 Streitfällen aus, in denen zunächst einmal kein krimineller Hintergrund zu vermuten ist.[587] Die dokumentierten Fälle reichen von falsch belasteten Konten bis hin zu Karten, deren Gebrauch, mit der Folge Bargeld zu erhalten, zu keiner Kontobewegung führt, und die Anderson spaßig ‚directors' cards' nennt.

Bis in die neunziger Jahre hinein hatten Banken, im Beispiel die englischen Banken, laut Anderson noch keine korrekte Prozedur zur Überprüfung implementiert, ob per Post versendete Karten und PINs auch tatsächlich beim Empfänger eingegangen waren oder in die Hände von Kriminellen geraten waren.[588]

Der Betrug durch Bankangestellte mit oder ohne Kooperation mit Kriminellen ist eine weitere Schadensquelle. Dabei werden in den bekannt gewordenen Fällen meist organisatorische oder technische Schwachstellen von den Tätern ausgenutzt. Beispielsweise hatte eine britische Bank für die Test- und Produktivumgebung ihrer Geldausgabeautomaten die gleichen kryptographischen Schlüssel verwendet, so dass korrupte Angestellte für gefälschte Karten mühelos PINs generieren und an interessierte Kreise verkaufen konnten.[589]

Anderson macht auf die besondere Bedeutung des Rechtssystems und die -kultur aufmerksam. Ein großer Teil der Angriffe auf britische (und auch norwegische) Geldausgabeautomaten konnte nur deshalb erfolgreich durchgeführt werden, weil es der Industrie über Jahrzehnte gelungen war, die Sicherheit ihrer Produkte als so hoch darzustellen, dass Irrtümer oder Angriffe gar nicht vorkommen könnten. In der Folge standen betrogene Kunden vor der Schwierigkeit, weder bei ihrer Hausbank noch bei Gericht überhaupt ernstgenommen zu werden.[590] Allerdings wurde diese Politik durch einige nachweisbare und öffentlich gewordene Betrugsfälle mit Geldausgabeautomaten in den 90er Jahren obsolet. In den USA hingegen wurde mit der Regulation E der Bankenaufsicht sogar eine Beweislastumkehr eingeführt: Banken haften für alle Fälle von Kartenmissbrauch, solange sie nicht den betroffenen Kunden betrügerische Aktivitäten nachweisen können. Die resultierenden Kosten gibt Anderson mit

[585] Schneier (2000), S. 380.
[586] Vgl. Buchmann (1999).
[587] Anderson (2001), S. 200.
[588] Anderson (2001), S. 201.
[589] Anderson (2001), S. 201.
[590] Anderson (2001), S. 201 und 203 f. Der gleiche Fall ungerechtfertigter Anklage wegen Betrug am Geldausgabeautomaten findet sich bei Schneier (2000), S. 40.

USD 15.000 pro Jahr pro Bank an und meint, diese Kosten wären tolerierbar und zudem drei Mal niedriger als die Kosten, die durch Vandalismus entstünden.[591] Auch in Frankreich wurde in Artikel 36 des „Everyday Security Act“ vom 15.11.2001 festgelegt, dass ein Kartenbesitzer nicht für Betrug mit seiner Karte durch Dritte haftbar gemacht werden kann. Ebenso wurden die Strafen für Kartenbetrug drastisch erhöht auf bis zu sieben Jahre Gefängnis und Strafen in Höhe von 750.000 Euro.[592]

Anderson listet noch eine Reihe weiterer Sicherheitsprobleme und Betrugsfälle bei Geldausgabeautomaten auf.[593] Ihnen ist gemeinsam, dass die Angriffswege vielfältig und teils unvorhersehbar waren, und nur ganz selten tatsächlich technisch ausgefeilte Methoden angewendet wurden, mit denen Computer- und Sicherheitsexperten gerechnet hatten. Besonders bezeichnend ist in dieser Hinsicht das Beispiel eines Geldausgabeautomaten, der aufgrund technischer Unzulänglichkeiten nach dem Einführen einer beliebigen Telefonkarte annahm, die letzte eingeführte Bankkarte wäre nochmals eingeführt worden. Durch Ausspähen der PIN konnten Angreifer sich am Konto des jeweils vorherigen Nutzers eines Automaten schadlos halten, ohne in Besitz der Originalkarte oder eines Duplikats sein zu müssen.

Grundsätzlich zeichnen sich eine Vielzahl von Schadensfällen durch Operationelle Risiken durch ihre schlechte Vorhersagbarkeit aus. Dabei ist nicht „nur“ die Problematik der Prognose einer Eintrittswahrscheinlichkeit gemeint, sondern die Schwierigkeit, potenzielle Angriffsstellen überhaupt zu identifizieren. Schneier verweist auf einen Fall im Januar 2003, bei dem durch den SQL-Slammer-Virus 13.000 Geldausgabeautomaten der Bank of America vorübergehend ausser Betrieb waren.[594] Dazu stellt Schneier selbstkritisch fest[595]:
„But before it happened, you couldn’t have found a security expert who understood that those systems were dependent on that vulnerability.“

Eine potenzielle Sicherheitslücke stellt das zunehmende Online-Angebot von Banken im Internet dar. Die Möglichkeiten, sich Zugang selbst zu SSL-geschützten Seiten zu verschaffen, und anschließend mit versteckten Befehlen Geld auf beliebige Kontos zu transferieren, ist mittlerweile praktisch demonstriert worden. Allerdings scheint sich in Teilen der Fachwelt eine gewisse Ernüchterung durchzusetzen. So stellt der Swedbank Sprecher Jesper Berggren fest[596]:
„Wenn der Mensch zum Mond fliegen kann, dann wird früher oder später auch jemand die Sicherheitssysteme umgehen können“.

In realer Umgebung gelang es dem von einer Bank beauftragten Lars-Olov Guttke, Deprotect, bei einem Angriff auf ihr Sicherheitsnetz, mit versteckten Befehlen Millionen von Dollar auf Testkonten zu verschieben, ohne dass der Angriff aufgefallen wäre. Guttkes Ansicht nach konzentrierten sich die Banken einseitig auf die Sicherung äußerer Zugänge, ohne die internen Systeme hinreichend zu überwachen.[597]

In der Polizeilichen Kriminalstatistik sind die erhobenen Zahlen wegen der vermuteten Dunkelziffer nur mit Vorsicht zu gebrauchen. Hinzu kommt eine Änderung der Gliederung bei Betrug mittels rechtswidrig erlangten unbaren Zahlungsmitteln, mit der Folge einer

[591] Anderson (2001), S. 203.
[592] Vgl. Beau (2002), S. 5.
[593] Vgl. Anderson (2001), S. 201 ff.
[594] Vgl. Schneier (2003).
[595] Schneier (2003).
[596] Handelsblatt (2002).
[597] Vgl. Handelsblatt (2002).

genaueren Untergliederung der einzelnen Betrugsarten. Eine Vergleichbarkeit mit den Zahlen der Vorjahre ist dadurch schwierig bis ausgeschlossen. Für eine Einschätzung des Schadensvolumens ist die Statistik nicht geeignet, da sie lediglich die Zahl an Betrugsdelikten, nicht aber die Schadenssumme erfasst (siehe Abbildung 10). Insgesamt wurden 2002 in Deutschland 6.507.394 Straftaten erfasst; der offiziell erfasste Betrug mit Zahlungsmitteln macht somit nur 1,7 % dieser Straftaten aus.

Betrug mittels rechtswidrig erlangter Zahlungsmittel 2002	116.344
Davon:	
Schecks	4.135
Debitkarten ohne PIN (Lastschriftverfahren)	40.346
Debitkarten mit PIN	36.969
Kreditkarten	29.326
Daten von Zahlungskarten	3.354
Sonstige unbare Zahlungsmittel	2.214

Abbildung 28: Polizeiliche Kriminalstatistik 2002: Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel

Auffallend ist der hohe Anteil an Betrug mit Debitkarten, in der Summe ist diese Art Betrug für 2/3 aller Schadensfälle verantwortlich. Kreditkarten, die in Deutschland allerdings auch eine deutlich geringere Verbreitung aufweisen als Debitkarten, machen ein weiteres Viertel der Betrugsfälle aus.

In der Öffentlichkeit wird aufgrund der hohen weltweiten Verbreitung die Kreditkartenzahlung im Internet kritisch betrachtet. Waren es zunächst unverschlüsselte Datenübertragungen, die leicht angreifbar waren, so sind kryptographische Methoden insbesondere die Secure Socket Layer-Verschlüsselung (SSL), die standardmäßig von Internet-Browsern unterstützt wird, heute Stand der Technik. Schadensfälle mit Kreditkarten lassen sich in verschiedene Kategorien einteilen:

Der Datenfluss im Internet wird abgefangen oder Server verschiedenster Teilnehmer im Einkaufsumfeld werden angegriffen; der Angreifer geht mit den erhaltenen Daten einkaufen und gibt zur Lieferung von Waren Adressen oder Wohnungen an, deren Bewohner später nicht nachvollzogen werden können. Erst mit den neusten Initiativen der Kreditkartengesellschaften, die zur Sicherung elektronischen Bezahlens nunmehr eingeführt werden – MasterCards „SecureCode“ und Visas „Verified by VISA“[598] – kann dieses Problem wirkungsvoll bekämpft werden. Bis dahin und bei nicht hinreichendem Einsatz von zusätzlichen Informationen wie CVV2 und CVC2 bleibt es ein Problem, falls Kreditkartendaten von Servern gestohlen werden. Anfang 2003 wurde ein großer Fall von gestohlenen Kreditkartendaten bemerkt. In den USA hatten Angreifer Zugang zum Server der Transaktions-Firma Data Processors International und gelangten in den Besitz von über acht Millionen Kreditkartennummern. Dieser Fall ist besonders bedenklich, da es sich nicht um irgendeinen kleinen ungeschützten Händler im Internet handelt, sondern um eine international tätige Firma, die mit der Überprüfung, Autorisierung und Weiterleitung von Kreditkarten-Transaktionen im Auftrag von Händlern ihr Geld verdient und die eigentlich gegen solche Angriffe geschützt sein müsste. Allerdings ist auch in diesem Fall (noch) nichts über entstandene Schäden berichtet worden.[599] Allerdings gehen Schätzungen von finanziellen Schäden, die durch

[598] Vgl. ausführlich 4.2.6.4.1.
[599] Vgl. Heise (2003a).

„Identitätsdiebstahl“ entstehen, für das Jahr 2003 von einer Größenordnung in der Höhe von rund 74 Mrd. US-$ aus, weltweit sollen es sogar 221 Mrd. US-$ sein.[600]

Betrug mit Kreditkarten kann zu hohen Chargeback-Raten führen, das heißt der Zahlungspflichtige weist die Zahlung, sobald er sie auf seiner Abrechnung findet, zurück. Drei Fälle lassen sich unterscheiden: a) durch Betrug Dritter, beispielsweise eine unbemerkt vom Besitzer gefälschte Karte, oder technische Probleme wurde das Kreditkartenkonto tatsächlich ungerechtfertigt belastet. Der entstehende Schaden geht zu Lasten der Kreditkartenorganisation oder des Händlers. b) der Zahlungspflichtige hat die Ware zwar erhalten, ist aber unzufrieden und weist die Bezahlung ab. In diesem Fall müssen Händler und Käufer eine Lösung finden, die Kreditkartenorganisation ist nicht betroffen. c) der Käufer gibt an, die Ware nicht erhalten zu haben. In diesem Fall liegt die Beweispflicht beim Händler, die Qualität seines Warenwirtschaftssystems und des Tracking-Systems des Lieferdienstes entscheiden, ob dem Käufer seine betrügerische Absicht nachgewiesen werden kann.

Die Chargeback[601]-Zahlen im Versandhandel, zu dem neben den Interneteinkäufen auch alle Geschäfte zählen, bei denen die Kreditkarte nicht physisch vorliegt, sind auf Dauer mit Werten zwischen 0,37 % und über 0,8 % aller Transaktionen in den ersten drei Quartalen 2002 immer noch zu hoch.[602] Andere Quellen gehen von noch höheren Werten im Bereich von 1,1% für das Jahr 2001 aus.[603] Im eCommerce liegen die Chargeback-Zahlen nach Angaben von Visa 14 mal höher als im Face-to-Face-Geschäft, bei dem die Karte physisch vorliegt. Visa geht nach eigenen Analysen bei Schadensfällen in diesem Bereich davon aus, dass lediglich bei 20 % der Streitfälle tatsächlich ein logistisches Problem oder Schwierigkeiten mit der Ware vorliegen. Die restlichen 80 % sind laut Visa Betrugsversuche.[604]

Für die Kreditkartengesellschaften ist eine öffentliche Diskussion um mangelnde Sicherheit nicht zuletzt wegen des Image-Verlustes kritisch. Visa zufolge ist das fehlende Vertrauen der Konsumenten in den Online-Handel ein Grund für weniger hohe Umsatzzahlen wie Aussagen bei VISA-Umfragen belegen:[605] „I know that I’m protected from fraud, but I just don’t want the hassle of having to claim back.“, „I’m scared that the merchant is disreputable and I won’t receive any goods.“, „Someone else might use my card to buy on-line, where no-one can check the signature panel.” Diese Annahme wird auch von anderen Autoren gestützt.[606] Noch kritischer sind negative Schlagzeilen für die Betreiber innovativer Verfahren; beispielsweise verunsichern Nachrichten über den Versuch, Passwörter für PayPal-Konten auszuspähen[607] Kunden und potenzielle Kunden unter Umständen so, dass sie auf „altbewährte“ Verfahren zurückgreifen.

Die Aussagen in der Online-Umfrage “Internet-Zahlungsverkehr aus Sicht der Verbraucher”, IZV6 aus dem Jahr 2003, stützen diese These jedoch nicht für die aktiven Einkäufer mit Kreditkarte, die sich sogar subjektiv sicherer fühlen als diejenigen Konsumenten, die nicht mit Kreditkarte im Internet einkaufen. Fast 70 % der Befragten, die bereits mit Kreditkarte eingekauft haben, fühlen sich im Internet sicher, gegenüber nur knapp 50 % derjenigen, die keine Kreditkarte zum Einkauf im Internet einsetzen.[608] Allerdings kann die These auch nicht

[600] http://www.aberdeen.com/ab_abstracts/2003/05/05030013.htm (09.09.2003).
[601] Rückgabe/Nichtakzeptanz einer Position in der Kreditkarten-Abrechung durch den Besitzer der Karte.
[602] Ovink (2002).
[603] Vgl. Gartner Group (2001).
[604] Vgl. Ovink (2002).
[605]Vgl. Ovink (2002).
[606] Vgl. Beau (2002), S. 3.
[607] Vgl. Heise (2002a).
[608] Vgl. Leibold (2003), S. 41.

widerlegt werden, da die Umfrage in der Regel keine hinreichend große Zahl an Nichtkäufern erreicht. Das subjektive Gefühl wird in der Umfrage überraschenderweise auch objektiv gestützt (siehe Abbildung 29).

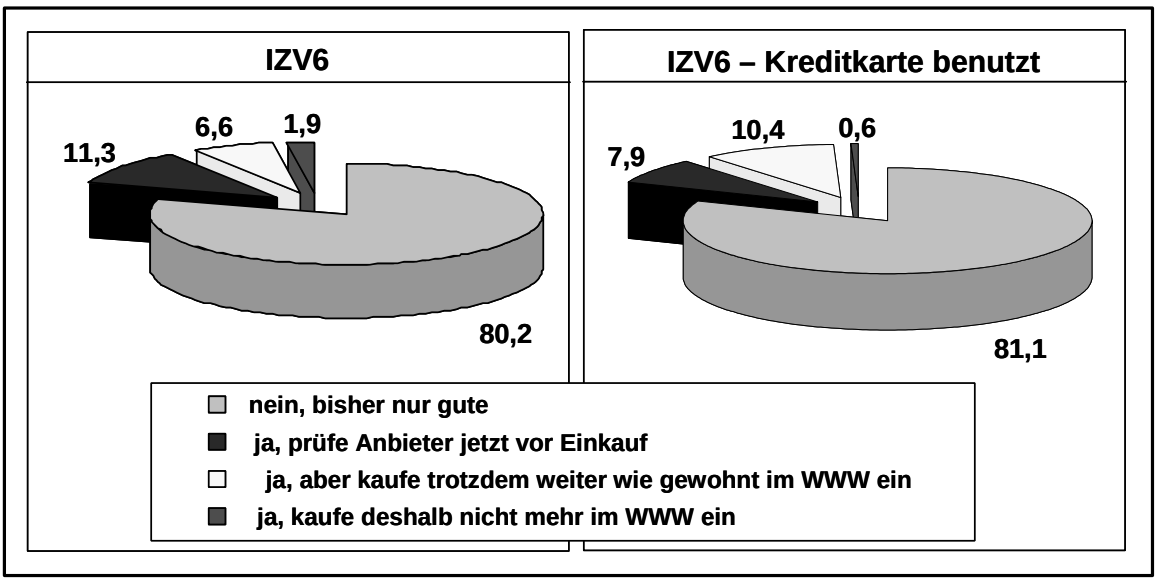

Abbildung 29: Internet-Zahlungsverkehr aus Sicht der Verbraucher: Haben Sie schon einmal negative Erfahrungen beim Bezahlen im Internet gemacht?[609]

Während bei den fast 10.000 Teilnehmern 1,9 % angeben, bereits mindestens einmal negative Erfahrungen beim Bezahlen im Internet gemacht zu haben, sind es in der Gruppe derjenigen, die zum Bezahlen auch die Kreditkarte benutzen, lediglich 0,6 %.

Ausgehend von amerikanischen Statistiken wird jedoch deutlich, dass in bestimmten Täterkreisen die Chancen von Betrug und Erpressung im und über das Internet erkannt worden sind. Auffällig sind die internationalen Dimensionen, in denen die folgenden Fälle sich abspielen.

Im Jahr 2001 wurden zwei Russen, Vasiliy Gorshkov und Alexey Ivanov, im besten Geheimdienstromanstil aus Chelyabinsk in Russland nach Seattle gelockt und dort festgenommen. Sie wurden in mehr als 20 Fällen für schuldig befunden, verschiedene Finanzinstitutionen, darunter die Nara Bank in Los Angeles, die Central National Bank in Waco und die Firma PayPal in Palo Alto, mittels Internet betrogen und erpresst zu haben.[610] Das Grundmuster aller Fälle bestand darin, sich von Russland aus über das Internet Zugang zu den Computern der verschiedenen Firmen – unter anderem Internet Service Provider, Auktionshäuser, eCommerce-Anbieter und Online-Banken – zu verschaffen und dann Kreditkarten- oder andere persönliche Finanzdaten zu stehlen. Im Zuge der Ermittlungen wurden auf den Rechnern der Täter 56.000 Kreditkartendaten und weitere Daten über diverse Online-Bank-Konten bei der Nara Bank und Central National Bank gefunden. Die Betrüger versuchten anschließend auf unterschiedlichste Art und Weise, ihr Wissen und den Zugang zu Firmennetzen auszunutzen:

Mit Hilfe sensibler Finanzinformationen versuchten sie verschiedene Institutionen zu erpressen, indem sie drohten diese Informationen zu veröffentlichen oder androhten, die Rechner der Opfer zu zerstören. Beim Zahlungssystemanbieter PayPal, der Zahlungen per

[609] Leibold (2003), S. 39.
[610] Vgl. Power (2002), S. 9 ff.

Email und Kreditkarte ermöglicht, gelang es den Tätern mit gestohlenen Kreditkarteninformationen Konten zu eröffnen und mit diesem Geld verschiedenstes Computerzubehör bei amerikanischen Händlern zu ordern. Computerprogramme ermöglichten den Tätern ferner, Tausende von Kunden- und Händlerkonten beim Online-Auktionshaus eBay zu eröffnen, die notwendigen Email-Adressen lieferten Provider kostenloser anonymer Email-Konten (Yahoo!, Hotmail etc.).[611] In der Folge konnten die beiden Täter bei eBay als Händler und Kunden auftreten und nach Belieben die Preise und den Ausgang von Auktionen manipulieren.

Der CSI/FBI-Report nennt diesen Fall exemplarisch und verweist auf ähnliche Fälle, in denen insbesondere Computerexperten aus der ehemaligen Sowjetunion weltweit betrügerisch agieren.[612]

Die Computer Business Review berichtet 2002 von einem Fall, bei dem ein 21-jähriger russischer Hacker namens Nicolai eine Bank in New York mit der Drohung erpresst hatte, sensible Daten aus ihrem eigenen Netz öffentlich zu machen.[613] Ihm war es gelungen, in das Firmennetz der Firma Online Resources Corp. einzubrechen, einer Firma, die Finanzdienstleistungen für Banken, unter anderem im Bereich eBanking und elektronische Rechnungsstellung, anbietet. Die Bank zahlte USD 10.000, nachdem Nicolai ihr Informationen über 1.500 Online-Konten zugeschickt hatte; den tatsächlichen Schaden beziffert die Bank auf USD 250.000. Der Mann wurde in Surgut, Westsibirien, nach Hinweisen der amerikanischen Polizei aufgrund der Rückverfolgung seiner IP-Adresse festgenommen.

Angriffe gegen Banken und Kreditkartenunternehmen erfolgen häufig indirekt. Anfang des Jahres 2000 wurde der Server eines Musiktitel-Anbieters, CDUniverse, mit Erfolg angegriffen.[614] Die Täter verschafften sich Zugang zu Kreditkarteninformationen und drohten für den Fall, dass sie keine USD 100.000 erhielten, mit der Veröffentlichung der Daten. Die betroffenen Kreditkartenunternehmen, American Express und Discover, ersetzten den Käufern, die auf der Seite von CDUniverse Musiktitel eingekauft hatten, insgesamt 300.000 Kreditkarten, um die Erpressung zu umgehen. Kosten der Aktion wurden nicht genannt.

In einem anderen Fall gelang es einem unbekannten Hacker, der sich Curador nannte, 26.000 Kreditkartendaten zu stehlen und sie auf einer Internetseite zu veröffentlichen. Der Schaden, der mit dieser Maßnahme ausgelöst werden könnte, wird vom FBI auf über USD 3 Mio. geschätzt.[615]

In Deutschland ist ein häufiges Problem von innovativen Zahlungssystemanbietern, die über das Internet agieren, weniger ein erfolgreicher Angriff auf die eingesetzte Technologie, sondern das der endgültigen Abrechnung zugrundeliegende Lastschriftverfahren.[616] Die neuen Verfahren sind im eigentlichen Wortsinn keine neuen Zahlungssysteme, eher neue Zugangsverfahren zu bereits existierenden Zahlungsverkehrsstrukturen. Als ein Beispiel kann an dieser Stelle Paybox, ein Anbieter von mobilen Bezahldiensten über das Mobiltelefon,

[611] An dieser Stelle helfen noch nicht einmal die Betrugspräventions-Maßnahmen, die eBay seit 2002 in Deutschland eingeführt hat. Demzufolge dürfen anonyme Email-Kontobesitzer nur noch dann ein eBay-Konto führen, wenn sie ihre Kreditkarteninformationen hinterlegen – bei gestohlenen Kreditkartendaten kein Sicherheitsgewinn.
[612] Vgl. Power (2002), S. 12.
[613] Vgl. Power (2002), S. 11 f.
[614] Vgl. Arnfield (2000), S. 11.
[615] Vgl. Arnfield (2000), S. 11.
[616] Experteninterviews haben ergeben, dass während der gesamten Laufzeit, die Paybox aktiv war, kein erfolgreicher Angriff auf technische Systeme stattgefunden hat.

genannt werden. In technischen Analysen war die Rede von möglicherweise geklonten SIM-Karten für das Mobiltelefon, in der Praxis waren in der Anfangszeit wohl tatsächlich hohe Rücklastschriften das tatsächliche Betrugsproblem.

Neue Verfahren müssen am Markt zunächst eine gewisse Bekanntheit erreichen, um einen Kundenstamm aufzubauen. Dabei wird zumindest in der Anfangsphase billigend in Kauf genommen, dass die Bonitätsüberprüfung neuer Kunden nur rudimentär ist, da sonst potenzielle Kunden abgeschreckt werden könnten. In der Folge spricht sich ein solches Verhalten bei möglichen Betrügern im Netz herum, und das schwächste Glied in der Zahlungskette sind dann keine technischen Finessen, sondern die Konditionen der Lastschrift. Diese kann nach den 2002 geänderten Allgemeinen Geschäftsbedingungen der meisten Banken (nur) noch sechs Wochen nach erfolgter Belastung des Kundenkontos widerrufen werden. Die Verfolgung einer solchen in betrügerischer Absicht durchgeführten Aktion ist zeitaufwändig, personalintensiv und damit teuer.

Eine weitere Möglichkeit, das System Paybox zu kompromittieren, ergab sich durch die Prozedur der Bestätigung einer erfolgten Paybox-Zahlung zwischen Paybox und Händler.[617] Auf der untersten Service-Level-Ebene für kleinere Online-Händler gab es bei Paybox die Möglichkeit, sich als Händler mit einer Email benachrichtigen zu lassen, wenn der Kunde eine Bezahlung per Paybox getätigt hatte. Diese Email war nicht verschlüsselt oder von Paybox signiert. Betrüger, die über diesen Sachverhalt Bescheid wussten, konnten in der Folge eigene Nachrichten an Händler generieren, mit der Mitteilung, für bestellte Waren sei die Zahlung bereits bei Paybox eingegangen beziehungsweise initiiert. Da der Händler de facto eine Zahlungsgarantie von Paybox ausgesprochen bekommen hatte[618], war der Geschädigte der Zahlungssystemanbieter Paybox, sofern es der Firma nicht gelang, auf dem Rechtsweg die Forderung einzutreiben.

Eines der Verfahren, die bislang als unangreifbar gelten, ist die vorausbezahlte Scratch-Karte. Bei diesen Karten für Kleinbetragszahlungen, Anbieter sind in Deutschland die paysafecard GmbH mit ihrer paysafecard und die Deutsche Telekom mit MicroMoney, wird eine 16-stellige PIN freigerubbelt, die beim ersten Einkauf eingegeben wird und ein Online-Konto freischaltet. Von diesem Konto wird bei jedem Einkauf nach Eingabe der PIN die gewünschte Summe abgezogen, bis sich kein Guthaben mehr auf dem Konto befindet. Die Übertragung der Nummer erfolgt verschlüsselt. Rein mathematisch ist ein Erraten aktiver Nummern so gut wie ausgeschlossen. Da zusätzlich für bereits aktivierte Karten noch ein Passwort vergeben werden kann, ist selbst für verlorene oder gestohlene Karten die Missbrauchsgefahr gering. Nach drei fehlerhaften Eingaben des Passworts wird die Karte gesperrt.

Auch bei den neusten elektronischen Zahlungssystemen, die eine gewisse Popularität unter anderem wegen des Erfolgs von internationalen Internet-Auktionen erreicht haben, wird von ersten Betrugsversuchen berichtet. Hintergrund ist die wie überall im Internet notwendige Authentifizierung eines Nutzers des Online-Bezahlsystems PayPal mithilfe eines Passworts. Ein Angreifer versuchte mittels einer gefälschten Internetseite, die die PayPal-Startseite imitierte, an die Zugangsdaten der Nutzer zu kommen, User-ID und Passwort.[619]

---

[617] Eigenes Erlebnis des Autors, der trotz erfolgter Paybox-Überweisung ungewöhnlich lange auf die Ware warten musste, und bei Recherchen vom Händler diese Betrugsmöglichkeit aufgezeigt bekam. Über die Höhe möglicherweise entstandener Schäden liegen dem Autor keine Kenntnisse vor.

[618] De jure kann ein Zahlungssystem-Dienstleister keine Zahlungsgarantie aussprechen. Dieses Geschäft ist ein Bankgeschäft. Der juristische Ausweg bestand in einem Forderungsaufkauf durch Paybox, bei dem der Händler seine Forderung an Paybox abtritt, und dafür die Forderung vollständig erstattet bekommt.

[619] Vgl. Hod (2002).

Noch weitreichender war der Versuch eines Versenders von Spam, der mit einer Mail versuchte, aktive PayPal-Nutzer zu einer gefälschten PayPal-Seite zu locken. Über die Zugangsdaten für PayPal hinaus sollten die Angeschriebenen auch noch ihre Adresse und die vollständigen Kreditkartendaten inklusive CVV-Nummern[620] angeben. Letzteres wäre bis zur Sperrung des Kreditkartenkontos besonders gefährlich, da diese Nummern als zusätzliches Sicherheitsmerkmal neben den reinen Kreditkartendaten beim Einkauf im Mail-order/Telephone-order Geschäft abgefragt werden und nicht auf den Servern des Händlers gespeichert werden (und somit auch normalerweise einem Angreifer im virtuellen Raum nicht bekannt wären).[621] In keinem der Fälle wurde allerdings anschließend von einem erfolgreichen Angriff auf Nutzerkonten berichtet.

Zunehmend werden indirekte Angriffe über das Internet bei neuen Vertriebskanälen von organisierten Banden durchgeführt. Diese Banden erweisen sich als sehr anpassungsfähig und nutzen die Problematik fehlender Authentifizierung, indem sie eine Art Mimikri betreiben. Die eigentlich für den Zweck der Vertrauensbildung gegründeten Treuhand-Services, die als unabhängige Dritte die Kaufabwicklung begleiten und das dem Verkäufer geschuldete Geld bis zur Freigabe durch den Käufer auf einem Treuhandkonto parken, werden perfekt imitiert. Möglich ist diese Imitation, da der Begriff Treuhandservice mittlerweile positiv beim Verbraucher besetzt, ist aber noch keine Markenidentifikation stattgefunden hat. Es wird geschätzt, dass 80 % der im Netz verfügbaren Treuhanddienste zum Zweck des Betrugs aufgebaute Anbieter sind, die technisch auf dem neuesten Stand ihre vermeintlichen Dienste anbieten.[622] Das Prinzip ist immer das Gleiche. Ware wird von einem eBay-Anbieter gekauft, mit Vorliebe teure Güter in höherer Anzahl. Der Betrüger beharrt auf einem Treuhanddienst seiner Wahl und erklärt sich sogar bereit die Kosten dafür zu übernehmen; der Verkäufer erhält die ungefälschte Mitteilung des betrügerischen Treuhanddienstes, das Geld sei eingegangen und schickt die Ware ab. Er erhält allerdings nie sein Geld. Die Gefahr, dass auch Zahlungssysteme von den Betrügern kompromittiert werden, ist besonders hoch, da sie bei der Registrierung beim gefälschten Treuhandservice die Passwortwahl des Betrugsopfers mitlesen können. Viele Internetnutzer greifen, nicht zuletzt wegen Überforderung durch eine hohe Anzahl Passwörter, auf ein begrenztes Kontingent an Passwörtern zu. Bei Wiederholungen riskieren beispielsweise Opfer eines Treuhandservices, die über ein eBay-Geschäft angezogen wurden, dass auch ihre eBay-Zugänge oder sogar die dazugehörigen Bezahlsysteme wie PayPal den Betrügern zugänglich werden.[623]

5.3.2.1.2 Operationelle Risiken und ausgewählte Schadensfälle im Großzahlungsverkehr

Der Großzahlungsverkehr ist international nicht zuletzt aufgrund der fachlich fundierten Arbeiten der Bank für Internationalen Zahlungsausgleich auf einem hohen Sicherheitsniveau. Gleichwohl gibt es einige dokumentierte Fälle, bei denen Angreifer verschiedene Schwachstellen ausnutzen konnten.[624] Allerdings sind die Täter in der Mehrzahl der öffentlich bekannt gewordenen Fälle aus den unterschiedlichsten Gründen gefasst worden.

---

[620] Card Verification Value, eine zusätzliche Prüfzahl, die auf der Rückseite von Kreditkarten aufgedruckt ist, und die elektronisch nicht ausgelesen werden kann. Somit muss zu deren Kenntnis die Karte physisch vorliegen.
[621] Vgl. Hod (2002).
[622] Vgl. www.sos4auctions.com/escrow/escrow.asp
[623] Vgl. o.V. (2003b).
[624] Thodén zufolge wurde ihr in Experteninterviews eine Schätzung für Londoner Finanzkreise genannt. Demnach werden dort pro Jahr fünf bis sechs betrügerische Überweisungen von Großbeträgen bei entsprechenden Versicherungen aktenkundig (Thodén (1999), S. 67 FN 48).

Einer der bekanntesten Fälle von Betrug im Großzahlungsverkehr geschah 1979. Stanley Rifkin, ein Berater, transferierte über USD 10 Mio. von der Security Pacific National Bank in die Schweiz. Er hatte als Berater einen Autorisierungscode für elektronische Überweisungen erspäht, der intern verwendet wurde. Dieser Code funktionierte entgegen klassischen Sicherheits-Richtlinien auch für eine per Telephon initiierte Überweisung. Er umging die Geldwäsche-Kontrollen, indem er von einer russischen Agentur in der Schweiz Diamanten kaufte. Lediglich seine Flucht nach dem erfolgreichen Transfer machte ihn verdächtig, ansonsten wäre er unter Umständen unentdeckt geblieben.[625]

Meist benötigen Innentäter beim Versuch, Großbeträge unter ihre Kontrolle zu bringen, auch entsprechende international agierende Komplizen. So gelang es 1993 einem Bankangestellten der NatWest in London mit Hilfe eines vom Kollegen erspähten Computer-Passworts, GBP 31,8 Mio. auf ein Bankkonto in Lugano, Schweiz, zu überweisen. Zwei Komplizen sollten das Geld in Lugano bar abheben. Der Betrug wurde nur deshalb aufgedeckt, weil die Geldsumme zu hoch war; wegen eines dem Täter unbekannten Limits in Höhe von GBP 20 Mio. überprüfte die Credit Suisse in Zürich den Transfer bei NatWest.[626]

Eine Variante des Betrugs, die sich auf sichere Nachrichtenformate im SWIFT-Netz stützt aber auch mit einer einfachen Urkunde und Empfehlungsschreiben funktioniert, ist eine gefälschte Bürgschaft einer Firma in einem Land für den Kredit einer Firma in einem anderen Land. Fällt der Bank, die die Bürgschaft akzeptiert, deren Fälschung nicht auf, ist der restliche Transfer von Geld völlig legal.[627] Thodén berichtet in ähnlichem Zusammenhang von zwei Fällen, die auf gefälschten Telex-Überweisungen beruhten: Im Dezember 1995 wurden von der Hongkong und Shanghai Banking Corporation (HSBC) in Jakarta USD 42 Mio. innerhalb von 3 Tagen mit drei verschiedenen Aufträgen zur Modern Bank und Unbind Bank in Indonesien transferiert. Die Aufträge schienen von neu eröffneten Konten einer italienischen Firmengruppe in Übersee-Filialen europäischer Großbanken, unter anderem der Dresdner Bank, zu kommen. Kurz nach dem Transfer wurden die Gelder in Dollar von den Tätern in Indonesien abgehoben. Eine daraufhin erfolgende Nachfrage bei der Hongkong Bank wurde trotz der hohen Summen von einfachen Angestellten positiv beschieden. Erst als die Hongkong Bank versuchte, ihrerseits die Gelder auf diesen Konten von den europäischen Banken zu erhalten, fiel der Betrug auf. Zu diesem Zeitpunkt hatten die Täter bereits USD 34 Mio. in bar ausgezahlt bekommen.[628]

In einem anderen Fall wurde 1996 eine betrügerische Transaktion in Höhe von USD 2,9 Mio. bei der Bank of Indonesia entdeckt. Dort hatte ein führender Manager mit zwei Untergebenen und zwei Komplizen außerhalb der Bank eine Empfangsbestätigung der dortigen Zentralbank gefälscht, mit der Anweisung, das Geld über die Bank of Indonesia an die ASEAM Indonesia Bank zu überweisen. Die Zentralbank bemerkte erst sechs Tage später die Unregelmäßigkeiten auf ihren Konten. Die Ermittlungen führten zwar zu den Tätern, allerdings blieb fast ein Drittel der Beute verschwunden.[629]

Bei einem weiteren Betrug gelang es im Februar 1997 einem Bankangestellten CHF 76 Mio. mit Hilfe gefälschter Telex-Anweisungen von einer Bank in Zürich zu einer niederländischen

[625] Vgl. Anderson (2002), S. 197. Eine geringfügig andere Version liefert Schneier (2000), S. 48: Schneier zufolge hatte Rifkin sogar die computergestützten Aufzeichnungen so manipuliert, dass keinerlei Auffälligkeiten mehr hätten gefunden werden können. Rifkin habe einem Anwalt von seiner Tat berichtet, der ihn dann angezeigt habe.
[626] Vgl. Thodén (1999), S. 67.
[627] Vgl. Anderson (2002), S. 196.
[628] Vgl. Thodén (1999), S. 68 f.
[629] Vgl. Thodén (1999), S. 67 f.

Bank in Lugano zu transferieren. Das Geld wurde von einem Komplizen weiter zu verschiedenen Banken in Monaco, Italien und Zypern geschickt, allerdings wurden die Täter gefasst, bevor ihnen Barabhebungen möglich wurden.[630]

Der Betrug wurde in den vorgenannten Fällen nicht durch das Überwinden komplexer Sicherheitsvorkehrungen beispielsweise der SWIFT-Formate oder kryptographischer Verfahren möglich, sondern durch das Zurückgreifen auf alternative vergleichsweise ungesicherte Wege. Und selbst wenn diese Wege mit entsprechenden Prozeduren abgesichert wären, zeigen die vorgenannten Fälle, dass deren Einhaltung nicht immer problemlos geschieht. Gerade der Aufbau komplexer Sicherheitsstrukturen für elektronische Abwicklungen und die Konzentration auf das Erlernen der notwendigen Mechanismen, lässt unter Umständen die Aufmerksamkeit in traditionellen Bereichen geringer werden.[631]

Schneier macht auf eine weitere Gefahr aufmerksam, die aus der Abhängigkeit der Banken von elektronischen Systemen und der Komplexität dieser Systeme basiert.[632] Seiner Ansicht nach wurden im Rahmen der Jahr 2000-Umstellungsarbeiten aus der Not heraus viele Programmierer mit Aufgaben an sicherheitskritischen Systemen beauftragt, die unter Umständen keine adäquate Sicherheitsüberprüfung durchlaufen hatten. Er befürchtet, einige Computerspezialisten hätten im Rahmen ihrer Tätigkeit Hintertüren in die Software einbauen können, oder Spionageprogramme zum Ausspähen von Passwörtern oder kryptographischen Schlüsseln. Auch wenn die These plausibel erscheint, lässt sich dazu (noch?) kein publizierter Fall finden.

Noch sind die Fälle betrügerischer Manipulation von Geldgeschäften über das Internet kein Massendelikt. Trotzdem gehen unterschiedliche Schätzungen für 1999 von American Bar Association, FBI und Europol von weltweiten Schäden durch internetbasierte Delikte im Zahlungsverkehr in der Größenordnung von zwei bis acht Mrd. US-Dollar aus.[633] Allein bei der jährlich stattfindenden Umfrage des Computer Security Institute wurden für 2002 Schäden durch „financial fraud“ in Höhe von über USD 115 Mio. genannt, von nur 25 befragten Unternehmen, die Zahlen nennen konnten und wollten![634]

Thodén skizziert einen der ersten Fälle eines computerbasierten Angriffs über ein Netzwerk.[635] 1994 gelang es einem russischen Wissenschaftler, Vladimir Levin, mit mehreren Komplizen von St. Petersburg aus, in das Netz der Citibankfiliale an der Wall Street einzubrechen und im Verlauf von 3 Monaten USD 10,7 Mio. an verschiedenste Konten bei unterschiedlichen Banken weltweit zu transferieren. Allerdings war einem Kunden der Citibank das Verschwinden von USD 200.000 bei einem der ersten Versuche aufgefallen, so dass die eingeschaltete Polizei die weiteren Einbrüche ins Netz beobachten und zurückverfolgen konnte. Angeblich wurden bis auf die ersten USD 400.000 alle weiteren Gelder zurückerstattet. Allerdings bleibt laut Thodén rätselhaft, wie Levin und Komplizen an die für die Transfers notwendigen Passwörter und Systemkenntnisse gekommen sind.

Die Gefahren, die Experten im Retail-Zahlungsverkehr sehen, sind bislang aufgrund der absoluten Höhe der einzelnen Zahlungen eher gering. Andererseits ändert sich diese Einschätzung, wenn Business-to-Business-Zahlungen berücksichtigt werden, da dann die

[630] Vgl. Thodén (1999), S. 69.
[631] Vgl. dazu auch Thodén (1999), S. 68 f.
[632] Vgl. Schneier (2000), S. 48.
[633] Thodén (1999), S. 69, FN 56.
[634] Vgl. Power (2002), S. 4, 10 ff.
[635] Thodén (1999), S. 69.

möglichen Schadenssummen in die Millionen gehen können.[636] Sofern jedoch die verwendete Technik die grundsätzlich gleiche ist, lohnt es sich bereits beim Retail-Zahlungsverkehr die Gefahrenlage richtig einzuschätzen. Zudem zeigen die oben skizzierten Fälle von internetbasierten Betrügereien und Erpressungen, dass mit dem Einbruch von Tätern in Bankennetze die Grenzen zwischen Retail- und Großzahlungssystemen zwar nicht verwischen, aber die Schadenssummen in beiden Systemen ähnliche Größenordnungen aufweisen können. Erschwerend wirkt im Fall der Retail-Systeme, dass auch die Sicherheitsmaßnahmen aufgrund der Masse der Zahlungen eher automatisiert sind. Kennen die Angreifer diese Maßnahmen kommen sie eher unentdeckt davon als im Fall der Großzahlungssysteme, bei denen eher noch aufgrund der kurzen Kommunikationswege Betrügereien aufgedeckt werden können.

Teilweise entscheidet jedoch der Rechtsrahmen über das Interesse von Banken an Sicherheitsmaßnahmen und ist somit für unterschiedliche nationale Sicherheitspolitiken verantwortlich. Beispielsweise haftet in der Schweiz der von Betrug betroffene Kunde beim Internet-Banking, sofern der Bank nicht fahrlässiges Handeln nachgewiesen werden kann. In Deutschland hingegen ist der Kunde bis zu einer geringen Summe nicht haftbar für betrügerische Handlungen mit seinem Konto, es sei denn, ihm kann (Mit-)Täterschaft nachgewiesen werden.

Eine Extremposition in Bezug auf die Haftungsproblematik nimmt Schneier ein.[637] Forderungen von Schneier gehen in die Richtung, die Haftung insbesondere für Software so zu gestalten, dass der Hersteller für alle Folgeprobleme haftet. Schneier schlägt dies spezifisch für sicherheitsrelevante Themen vor und meint, ein gut Teil der existierenden Probleme würde sich damit erübrigen.

Sicherheit als Prozess verstanden, führt weniger zu dem Problem, dass ein einmal erreichter Zustand als befriedigend angesehen wird. Vielmehr wird gerade aufgrund technologischer Entwicklungen ein ständiges Überprüfen bestehender Sicherheitsmechanismen und –paradigmen notwendig, um erfolgreich den ebenfalls aufrüstenden Angreifern gegenübertreten zu können. Die aufgeführten Beispiele haben ferner verdeutlicht, dass rein technische Sicherheitslösungen selten ausreichend sind. Gerade das Überwinden verschiedener Kontrollmechanismen durch Ausweichen der Angreifer auf die nächsten Ebenen der Sicherheit, beispielsweise auf die juristische Ebene, wie sie im Schalenmodell beschrieben sind, führt zu erfolgreichen Angriffen.

5.3.2.1.3 Ansätze zur Identifikation und Klassifikation von Risiken im Zahlungsverkehr

Die BIZ gibt mit dem 4. Grundsatz der „Sound Practices for the Management and Supervision of Operational Risk“ den Rahmen vor, in dem sich zukünftig die Identifizierung und auch Klassifikation Operationeller Risiken bewegen wird[638]: „Banks should identify and assess the operational risk inherent in all material products, activities, processses and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.”

Die BIZ betont in ihren Ausführungen die Bedeutung der sachgerechten Identifizierung Operationeller Risiken als Grundlage jedes Risikomanagements. Dabei sollen von den

[636] Vgl. Thodén (1999), S. 69 ff.
[637] Vgl. Schneier (2000), S. 363 ff.
[638] BIZ (2003a), S.8.

Banken neben internen Faktoren und Entwicklungen auch externe Entwicklungen wie technischer Fortschritt und Marktveränderungen mit berücksichtigt werden. Eine weitere Herausforderung an das Risikomanagement stellt die geforderte Berechnung der Risikoexponiertheit einer Bank bezüglich der identifizierten Risiken dar.[639]

Für die Identifizierung der Operationellen Risiken macht die BIZ keine spezifischen Vorgaben, sondern listet zunächst alternative Möglichkeiten auf. Dieses Vorgehen resultiert aus fehlenden Erfahrungswerten in der Vergangenheit. Durch einen zugelassenen „Wettbewerb" der Methoden in der Praxis soll die Bewertungsfrage einzelner Verfahren einfacher zu beantworten sein, wenn erste valide Daten vorliegen. Unter den genannten Ansätzen befinden sich:[640]

- Risiko-Untersuchungen, bei denen die Banken ihre Risikoposition gegenüber bekannten Operationellen Risiken in internen Prozeduren selbst evaluiert (self assessment). Dabei können Checklisten, Workshops oder Scorekarten zur Bewertungsfrage eingesetzt werden.
- Risk Mapping: Es werden analog zu den Kategorisierungsvorstellungen der BIZ[641] die einzelnen Geschäftsbereiche bis hinunter zu einzelnen Aktivitäten und Prozessen in Risikoklassen/-typen eingeteilt, die auf den ersten Blick Schwachstellen erkennen lassen.
- Risiko-Indikatoren, beispielsweise Personalfluktuation oder Systemausfallraten, können zur Risikofrüherkennung sowie zur Kontrolle eingesetzt werden.
- Messsysteme, die aufbauend auf historischen Daten den Aufbau einer Datenbank für Operationelle Risiken erlauben. Dabei ist die Feinabstufung bei der Erfassung einzelner Schadensfälle beispielsweise Häufigkeit, Schadenshöhe, Ursachen etc. den Banken überlassen.

Eine ausführliche Diskussion der verschiedenen Ansätze zur Identifizierung findet sich u.a. bei Simon und Hofmann.[642] Im Ergebnis werden Risiko-Indikatoren als handhabbare Lösung dargestellt, während die komplexere Prozessanalyse mit formalen Fehlerbaumanalysen den als kritisch identifizierten Teilprozessen überlassen bleiben sollte. Die im Rahmen der quantitativen Abschätzung Operationeller Risiken von der BIZ gewonnenen Daten können anhand realisierter Schadensfälle einen ersten Eindruck vermitteln, welche Bereiche einer genaueren Untersuchung bedürfen.[643]

Der Schwerpunkt der Ansätze in Basel II liegt bislang erkennbar auf der Quantifizierung der Operationellen Risiken. Lediglich wenn es gelingt, eine hinreichende Vergleichbarkeit der Daten zwischen Banken herzustellen, und in einigen informationstechnologischen Bereichen eventuell darüber hinaus auch mit anderen Branchen, kann aus aufsichtlicher Sicht das Ziel erfüllt werden, eine risikoadäquate Eigenkapitalunterlegung herbeizuführen.

Einen wichtigen Schritt ist die BIZ mit der Einführung sogenannter „Operational Risk Data Collection Exercises" (auch „Loss Data Collection Exercise" (LDCE) genannt) gegangen. Hintergrund empirischer Datenerhebungen bei internationalen Banken war dabei das Bemühen, die generellen Auswirkungen des Basel II Konstrukts auf den Markt besser einschätzen zu können; vor dem tatsächlichen Anwendungsjahr 2006. In diesem Zusammen-

[639] Vgl. BIZ (2003a), S. 8, Ziffer 23 f.
[640] BIZ (2003a), S. 8 f, Ziffer 25.
[641] Vgl. BIZ (2002b), Annex 1.
[642] Vgl. Simon (2002), S. 129 – 142 und Hofmann (2002b), S. 25 ff.
[643] Vgl. ausführlich Abschnitt 5.3.2.2.

hang wurden die „Quantitative Impact Studies“ (QIS) durchgeführt, bei denen in der jüngsten im Oktober 2002 gestarteten und im April 2003 abgeschlossenen Studie QIS3 Banken aus 43 Ländern teilgenommen hatten; 188 Banken aus den 13 Mitgliedsländern des Basler Ausschusses für Bankenaufsicht und weitere 177 Banken aus 30 anderen Ländern.[644] Die fortgeschrittenen Ansätze wurden allerdings lediglich von den international tätigen Großbanken angewendet, die Zahl dieser teilnehmenden Banken lag bei 57 Banken.

Entscheidend ist für den Aufbau eines Risikomanagements Operationeller Risiken unter Qualitätsgesichtspunkten eine einheitliche Identifizierung und Kategorisierung der Risiken. Der Ansatz der BIZ zunächst die Aktivitäten der Bank ausgehend von Geschäftseinheiten auf Geschäftsbereiche und dann einzelne Unternehmensaktivitäten herunterzubrechen (siehe Tabelle 9), erscheint erfolgversprechend für ein systematisches und standardisiertes Vorgehen.

Business Unit	**Business lines** **Level 1**	**Level 2**	**Activity Groups**
INVESTMENT BANKING	Corporate Finance	Corporate Finance	Mergers & Acquisitions, Underwriting, Research, Privatisations, IPO, Securitisations, etc.
		Municipal/Government Finance	
		Merchant Banking	
	Trading & Sales	Advisory Services	
		Sales	Fixed Income, equity foreign exchange, commodities brokerage debt etc.
		Market Making	
		Proprietary Positions	
		Treasury	
BANKING	Retail Banking	Retail Banking	Retail lending and deposits, bank. services etc.
		Private Banking	Private lending and deposits, trust and estates etc.
		Card Services	Merchant/Commercial/Corporate cards, private labels and retail
	Commercial Banking	Commercial Banking	Project finance, real estate, export finance, trade finance etc.
	Payment and Settlement[645]	External Clients	Payments and collections, fund transfer, clearing and settlement
	Agency Services	Custody	Escrow, Depository Receipts, Corporate actions etc.
		Corporate Agency	Issuer and paying agents
		Corporate Trust	
OTHERS	Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open etc.
		Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open etc.
	Retail Brokerage	Retail Brokerage	Execution and full service

Tabelle 9: Klassifizierung von Unternehmensaktivitäten nach Basel II[646]

Grau hinterlegt ist der Bereich, in dem vorwiegend elektronischer Zahlungsverkehr abgewickelt wird.

[644] Vgl. BIZ (2003f), S 1 f.
[645] BIZ (2002b), Annex 1: „Payment and settlement losses related to a bank’s own activities would be incorporated in the loss experience of the affected business line.”
[646] BIZ (2002b), Annex 1.

In einem nächsten Schritt werden Verlustereignistypen kategorisiert (siehe Tabelle 10). Mit der Kombination dieser vorgeschlagenen Untergliederung der Finanzinstitute bis auf die Ebene der Geschäftsaktivitäten mit den potenziellen Schadensklassen oder –ereignistypen besteht nunmehr erstmalig die Gelegenheit ein Risikomanagement unter dem Gesichtspunkt der Vergleichbarkeit und damit der Qualitätssicherung und Überprüfbarkeit aufzubauen.

Grundsätzlich scheint von der BIZ mit diesem Vorgehen auch die Frage beantwortet, ob „bottom up"-Ansätze (Aggregation einzelner Schadensfälle) oder „top down"-Methoden (Festlegung von Risikokennzahlen auf Bereichsebene und Herunterbrechen auf Geschäftsfelder) erfolgversprechender zu sein scheinen. Die Nachteile der nicht auf die einzelnen Geschäftsprozesse eingehenden „top down"-Verfahren, z. B. des Capital Asset Pricing Models (CAPM), bei dem anhand der Entwicklung der Aktienkurse versucht werden kann, die Bedeutung Operationeller Risiken zu ermessen, überwiegen die Vorteile, beispielsweise das einfachere und kostengünstigere Vorgehen.[647] Die BIZ favorisiert klar einen „bottom up"-Ansatz.

Es zeigen sich allerdings bereits die Grenzen des von der BIZ vorgeschlagenen Kategorisierungsansatzes. Beim Zahlungsverkehr werden nur Dienstleistungen für Kunden bei der Kategorisierung berücksichtigt.[648] Schadensfälle im Zahlungsverkehr, die aus Geschäftsvorgängen innerhalb der Bank resultieren, sollen bei der jeweiligen Geschäftseinheit verbucht werden. Aus Sicht einer ordnungsgemäßen Zuordnung eines Schadensfalls zur betroffenen Kostenstelle ist dieses Vorgehen folgerichtig. Nicht geeignet erscheint es für den Überblick, in welcher Größenordnung einzelne Bereiche wie der Zahlungsverkehr Schäden erlitten haben. Ebenso ist es für die auf den Schaden folgende Analysephase unter Umständen vorteilhaft, wenn einzelne interne Fälle, welche die gleiche Schadensursache haben können wie Fälle, bei denen externe Kunden berührt werden, der gleichen Kategorisierungsgruppe zugeordnet werden.

Eine ähnliche Problematik gilt für den Bereich der Operationellen Risiken, die bisher bei den Kreditrisiken berücksichtigt wurden. Die BIZ möchte zunächst diese Zuordnung nicht ändern, aber gleichwohl die erkannten Risiken bei den Operationellen Risiken – allerdings nicht monetär berücksichtigt – aufführen.[649]

Neue Produkte im Bereich der Kreditrisiken haben teilweise Risiken aus dem Kreditbereich in den Bereich Operationeller Risiken transferiert, beispielsweise die Verminderung von Kreditrisiken durch Securitisation. Sofern das innewohnende Operationelle Risiko nicht berücksichtigt wird, z. B. die Abwicklungsrisiken, ist der Eindruck einer vollständigen Risikoreduktion nicht korrekt.

[647] Vgl. ausführlich Peter (2000), S. 658 ff.
[648] Vgl. BIZ (2003f), Annex 1, FN. 1.
[649] Vgl. BIZ (2003d), S. 128.

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal Fraud (I)	losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party	Unauthorised Activity	Transaction not reported (intentional) Transaction unauthorised (w/monetary loss) Mismarking of position (intentional)
		Theft and Fraud	Fraud/credit fraud/worthless deposits Theft/extortion/embezzlement/robbery, Misappropriation of assets Malicious destruction of assets, Forgery/Check kiting/Smuggling Account take-over/impersonation/etc., Tax non-compliance/evasion (wilful), Bribes/kickbacks, Insider trading (not on firm's account)
External Fraud (II)	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery Check kiting
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety (III)	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events	Employee Relations	Compensation, benefit, termination issues Organised labour activity
		Safe Environment	General liability (slip and fall, etc.) Employee health & safety rules events Workers compensation
		Diversity & Discrimination	All discrimination types

Tabelle 10: Klassifizierung möglicher Verlustereignisse[650]

(Fortsetzung nächste 2 Seiten), Mögliche Schadensfälle oder Risiken, die spezifisch auf elektronischen Zahlungsverkehr zutreffen, sind in der Tabelle hellgrau unterlegt.

[650] BIZ (2002b), Annex 2. Die römischen Ziffern korrespondieren zu den Resultaten des Entscheidungsbaums in Abbildung 30.

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Clients, Products & Business Practices (IV)	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitabilitiy requirements), or from the nature or design of a product	Suitability, Disclosure & Fiduciary	Fiduciary breaches/guideline violations Suitability/disclosure issues (KYC, etc.) Retail consumer disclosure violations Breach of privacy, Aggressive sales, Account churning Misuse of confidential information, Lender Liability
		Improper Business or Market Practices	Antitrust, Improper trade/market practices, Market manipulation Insider trading (on firm's account), Unlicensed activity Money laundring
		Product Flaws	Product defects (unauthorised, etc.) Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Acitivities	Disputes over performance of advisory activities
Damage to Physical Assets (V)	Losses arising from loss or damage to physical assets from natural disaster or other events	Disaster and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business Disruption and System Failures (VI)	Losses arising from disruption of business or system failures	Systems	Hardware, Software Telecommunications Utility outage/disruptions

Tabelle 11: Klassifizierung möglicher Verlustereignisse (Fortsetzung)

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Execution, Delivery & Process Management (VII)	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	Miscommunication, Data entry, maintenance or loading error Missed deadline or responsibility Model/system misoperation Accounting error/entity attribution error Other task misperformance, Delivery failure Collateral management failure, Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation
		Customer Intake and Documentation	Client permissions/disclaimers missing Legal documents missing/incomplete
		Customer/Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty misperformance Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing, Vendor disputes

Tabelle 11: Klassifizierung möglicher Verlustereignisse (Ende)

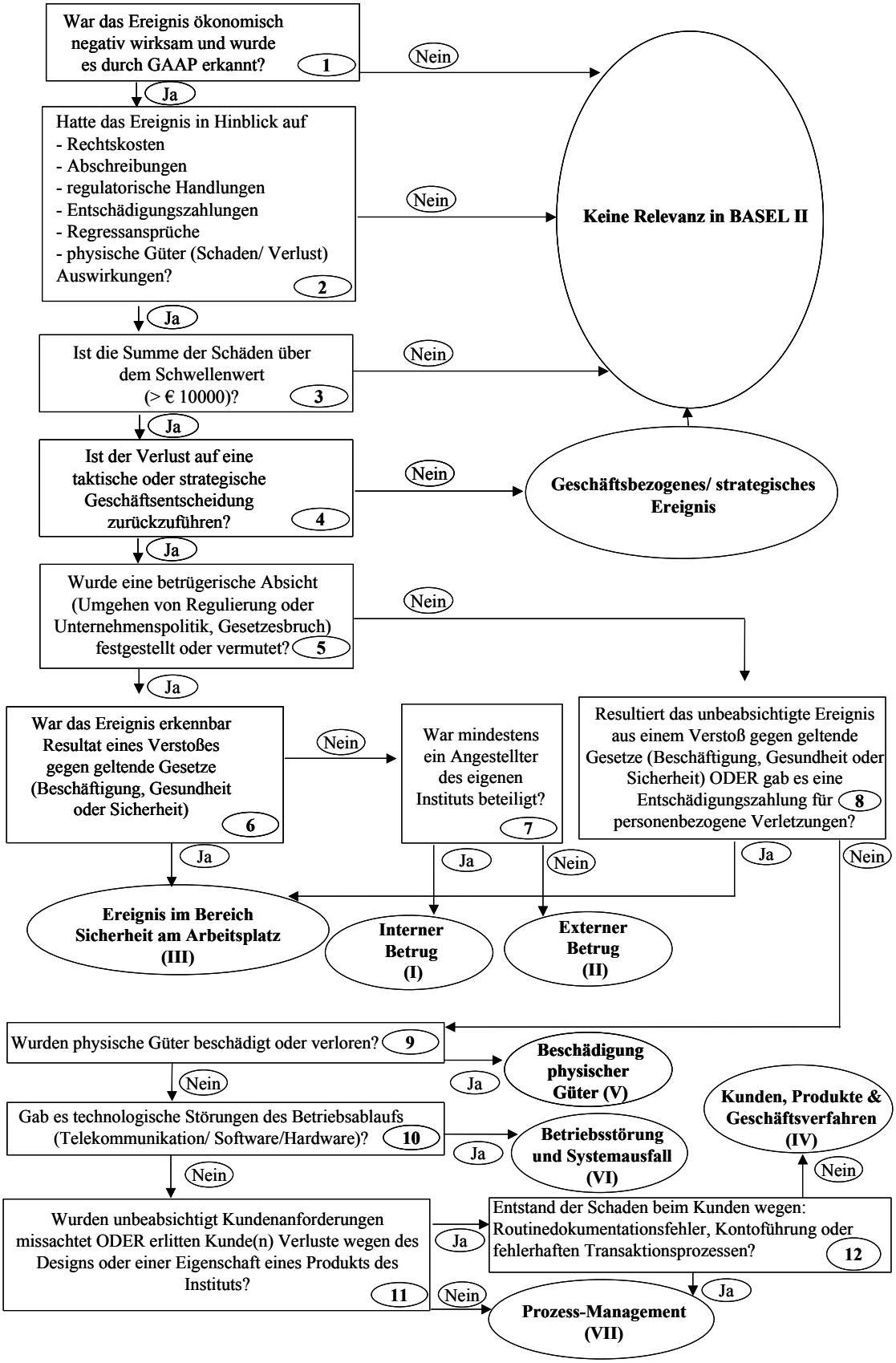

Abbildung 30: Entscheidungsbaum: Klassifikation der Schadensfälle nach Basel II[651]

[651] Vgl. BIZ (2002b), Annex 2, Tabelle 2, Übersetzung durch den Autor, leicht modifiziert, inhaltlich unverändert. Die römischen Ziffern in Klammer entsprechen der Schadensfallkategorisierung in Tabelle 9. GAAP: Generally Accepted Accounting Principles.

Positiv ist der Versuch der BIZ zu werten, eine eindeutige Kategorisierung mit einem vorgegebenen Entscheidungsbaum (siehe Abbildung 30) zu unterlegen – bei fortschreitenden Erhebungen kann die Erfassung softwarebasiert unterstützt werden. Die konsequente Kategorisierung ist nicht nur für die mögliche Quantifizierung der Risikoarten von Bedeutung, sondern ermöglicht darüber hinaus im nächsten Schritt die Schadensanalyse erheblich.

Der Anreiz für die Finanzinstitute, ein aufwändiges Risikomanagement für Operationelle Risiken aufzubauen und zu implementieren, sollte nicht allein aus dem regulatorischen Imperativ resultieren, sondern den Unternehmen auch die Vorteile eines solchen Vorgehens für (zukünftige) Betriebsergebnisse verdeutlichen. Bei der geltenden Konzentration auf die (notwendige) Frage der Quantifizierung Operationeller Risiken geraten diese möglichen Vorteile in der Argumentation in den Hintergrund.

Der regulatorische Druck, die fortgeschrittenen Ansätze zu verwenden, ist zumindest für kleinere und spezialisierte Institute, die in den QIS in der Gruppe 2 geführt werden (Gruppe 1: „Tier 1 capital" > € 3 Mrd., Gruppe 2: „Tier 1 capital" < € 3 Mrd.[652]), offensichtlich nicht sehr hoch.[653] Sie haben die Möglichkeit, auf den Basisindikatoransatz, den Standardansatz oder den alternativen Standardansatz auszuweichen und machen davon so ausgiebig Gebrauch, dass für die QIS3 nur ungefähr ein Achtel der teilnehmenden Banken aussagefähige Daten über fortgeschrittene Ansätze im Operationellen Risikomanagement liefern (können). Von 365 Banken konnten bei QIS3 nur 89 genaue Angaben zu quantifizierten Schadensfällen im Operationellen Risiko machen. Von diesen wiederum konnten die Daten von 32 Banken vollständig ausgewertet werden, der Rest hatte teilweise erhebliche Mängel, beispielsweise war keine (vollständige) Klassifikation der Schadensfälle möglich oder die Schwellenwerte für die Schadensmeldung waren von € 10.000 verschieden.[654] Diese Kritik an der Datenqualität zieht sich wie ein roter Faden durch die Quantitative Impact Studies. Bereits 2001 kam der Baseler Ausschuss für Bankenaufsicht bei der Analyse der Gesamtdaten aus den Jahren 1998 –2001 in Bezug auf die Auswirkungen von Basel II auf die Finanzinstitute zum Schluss: „[...], although supervisors have worked hard to try to verify the results, there remain significant questions over the quality of data. Banks have found it difficult, if not impossible in some cases, to overcome data limitations."[655]

Allen Beschränkungen zum Trotz werden neue Verfahren für das Management Operationeller Risiken sich an den Anforderungen von Basel II orientieren müssen. Dabei gibt es einerseits die Option, passiv auf die Entwicklung zu reagieren, oder andererseits offensiv mit der Aufsicht in dem von ihr angestrebten Dialog die Entwicklung mit zu prägen. In Kapitel 5.3.3 wird aufbauend auf dem von Basel II vorgegebenen oben dargestellten Rahmen ein Ansatz vorgestellt, der zwar intensiver in der Erhebungsphase ist, gleichwohl aber einen signifikanten Zusatznutzen bei der Auswertung der resultierenden Daten verspricht.

5.3.2.2 Bewertung Operationeller Risiken

Die „Sound Principles"[656] betonen zwar die Rolle der Identifizierung und Bewertung von Risiken, beschränken ihre Ausführungen in diesem Bereich aber nur auf Grundsatz 4.[657] Die Quantifizierung wird dort in einem Unterpunkt eher als Feststellung des Status Quo der

[652] BIZ (2003h), S. 1.
[653] Vgl. BIZ (2003g), S. 2.
[654] Vgl. BIZ (2003f), BIZ (2003g).
[655] BIZ (2001k), S. 6.
[656] BIZ (2003a).
[657] BIZ (2003a), S. 8 f.

Risikoquantifizierung durch Finanzinstitute denn als Empfehlung für den Einsatz bestimmter Verfahren vorgenommen.

Die BIZ stellt fest, dass von den Finanzinstituten eine ganze Reihe von verschiedenen Verfahren angewendet werden, um das Ausmaß Operationeller Risiken zu erheben. Die Berechnungen können auf historischen Schadensfällen basieren. Die BIZ schlägt vor, systematisch die Häufigkeit, den Schweregrad und andere relevante Informationen über jeden einzelnen Schadensfall zu erfassen. Dabei können die Informationen über interne Schadensfälle mit externen Schadensdatenbanken, der Szenarioanalyse und Risikobewertungsfaktoren kombiniert werden.[658]

Die Festlegung auf bestimmte Verfahren wird durch die mögliche Quantifizierung Operationeller Risiken für die resultierende Eigenmittelunterlegung vorgegeben. Grundsätzlich kann zwischen bankinternen und aufsichtlich zugelassenen Messverfahren unterschieden werden (siehe Tabelle 11). Es kann aber davon ausgegangen werden, dass sich mittelfristig nur die von der Aufsicht anerkannten Messverfahren durchsetzen werden. Basel II wird durch die vorgesehene Anwendung auf de facto alle Finanzinstitute im europäischen Raum die Notwendigkeit mit sich bringen, ein geeignetes Risikomanagement aufzubauen.

Bankinterne Messverfahren	**Aufsichtlich zugelassene Messverfahren**	**Ausprägungen der zugelassenen Verfahren**
Szenarioanalyse	Basisindikatoransatz	Basisindikatoransatz mit aufsichtlich vorgegebenem Risiko-Faktor α
Sensitivitätsanalyse	Standardansatz[659]	Standardansatz mit aufsichtlich vorgegebenem Risiko-Faktor β
Drei-Werte-Verfahren		Alternativer Standardansatz mit zusätzlich vorgegebenem Faktor m
Elastizitätskonzept	Fortgeschrittene Messverfahren	Keine Präferenz für einzelne Verfahren aber detaillierte Vorgaben[660], u.a. Aufbau interner Schadensfälle-Datenbank Intergration externer Datenbanken Szenarioanalyse
Risikomessung mit Hilfe annualisierter Gesamterwartungswerte		
CAPM-basierter Ansatz		
Value-at-Risk (VaR)		

Tabelle 11: Messverfahren zur Quantifizierung Operationeller Risiken[661]

Beim gegenwärtigen Entwicklungsstand dieses speziellen Gebiets innerhalb der Bankenlandschaft kann erwartet werden, dass die Institute nur von der Aufsicht (voraussichtlich) anerkannte Verfahren implementieren werden. Die Finanzinstitute haben bei der Wahl der geeigneten Verfahren die Möglichkeit, sich bei der Datenerhebung im Rahmen der „Quantitative Impact Studies“ und der Konsultationen zu beteiligen, und die Auswahl der letztendlich zugelassenen Verfahren mitzubestimmen. Performante bankinterne Messverfahren haben bei diesem Prozedere die Chance als aufsichtlich anerkannte Verfahren zugelassen zu werden. In der Risikomanagement-Literatur wird davon ausgegangen, dass sich der „Operational Value

[658] BIZ (2003c), S. 9.
[659] Zusätzlich müssen qualitative Kriterien an das Risikomanagement erfüllt sein. Vgl. BIZ (2003d), S. 124 f.
[660] Zusätzlich müssen qualitative und quantitative Kriterien an das Risikomanagement erfüllt sein. Vgl. BIZ (2003d), S. 125 f.
[661] In Anlehnung an Hofmann (2002b), S. 55; eigene Ergänzungen.

at Risk“-Ansatz, der analog zu den Verfahren im Markt- und Kreditrisikobereich aufgebaut ist, zu Zwecken der Gesamtrisikosteuerung durchsetzen wird.[662]

5.3.2.2.1 Basel II und Schadenspotenzial durch Operationelle Risiken

Das Risiko für Verluste durch Schadensfälle im Bereich Zahlungsverkehr ist bei weitem geringer als das Risiko der Banken im seit langem adressierten Marktrisiko- oder Adressausfallbereich. Beispielsweise geht Artopoeus in seinem Vortrag zu „Kreditrisiken aus bankaufsichtlicher Perspektive“ davon aus, dass allein in Deutschland in den letzten 40 Jahren ungefähr 100 private Banken aufgrund von Kreditverlusten insolvent geworden sind.[663] Allerdings sieht er die Kreditrisiken nicht nur im traditionellen Finanzierungsbereich, sondern er erkennt ein erhebliches Verlustpotenzial bei den Adressen- oder Erfüllungsrisiken im Handelsgeschäft der Banken, im Interbankengeschäft, in Geld- und Kapitalanlagen aber auch im Zahlungsverkehr.

Gleichwohl betont der Basler Ausschuss für Bankenaufsicht, dass Operationelle Risiken einen wichtigen Risikofaktor für Banken darstellen.[664] Im Übrigen sind einige der zur Zeit bei den Kreditrisiken verbuchten Risiken durchaus Operationelle Risiken, sie sind nur nicht als solche benannt, da diese Kategorisierung bislang nicht zur Verfügung stand.[665]

Bei Expertenbefragungen wird Operationellen Risiken ebenfalls ein hohes Gefahrenpotenzial zugestanden. In einer Umfrage unter britischen Banken im Jahr 1997 schätzten zwei Drittel der Befragten die Bedeutung dieser Risiken als mindestens gleichbedeutend wie Markt- oder Kreditrisiken.[666] Es zeigt sich bei der subjektiven Wahrnehmung der Akteure, dass Risiken, die kaum greifbar sind, und dadurch nicht beherrschbar werden, signifikant bedrohlicher empfunden werden, als erste empirische Daten dies vermuten lassen.

Die Gefahr systemischer Schäden durch terroristische Angriffe wird unterschiedlich beurteilt. Wird wie beim New Yorker Angriff am 11. September 2001 in großem Maße Infrastruktur beschädigt, sind Schäden kaum zu vermeiden. Die amerikanischen Aufsichtsbehörden kommen in ihrer Analyse zum Schluß, dass gegen solche Risiken weitreichende Maßnahmen insbesondere bei Zahlungssystemen von herausragender Bedeutung für die Volkswirtschaft, also hauptsächlich Großzahlungssysteme, ergriffen werden müssten.[667] Schneier hingegen kommt bei der Betrachtung der Schäden durch Cyberterrorismus zur nüchternen Einschätzung, dass das notwendige Wissen entsprechend dimensionierte Schäden anzurichten weder auf der Seite der Terroristen noch auf der Seite der Sicherheitsexperten vorhanden wäre[668]: „We simply don’t understand the interaction well enough to predict which kinds of attacks could cause catastrophic results, and terrorist organizations don’t have that sort of knowledge either – even if they tried to hire experts.“ Schneier leugnet nicht, dass es Angriffe auf die entsprechenden Netze geben kann, spricht jedoch statt von Cyberterrorismus von Cyberhooliganism und betont, die wahren Gefahren drohten eher durch kriminelle Handlungen wie Betrug und Spionage als durch Terror.

---

[662] Vgl. u.a. Hofmann (2002b), S. 59 ff., Jörg (2002), S. 73 ff., Simon (2002), S. 148 f., Stocker et al. (2001). Kritisch hierzu Anders (2001), S. 445.
[663] Vgl. Artopoeus (1998).
[664] Vgl. BIZ (2002k), S. 1, Ziffer 5.
[665] Vgl. BIZ (2003d), S. 128.
[666] Vgl. Thodén (1999), S. 15 f. Die Umfrage, auf die sie sich bezieht: British Bankers’ Association/ Coopers & Lybrand (Hrsg) (1997): 1997 Operational Risk Management Survey, The British Bankers’ Association and Coopers & Lybrand, London.
[667] Vgl. Board of Governors (2002).
[668] Schneier (2003).

Im Januar 2001 ging der Basler Ausschuss für Bankenaufsicht in den Beratungsunterlagen zum Thema Operationelles Risiko nach Sichtung der ersten verfügbaren Daten von einer Unterlegung Operationeller Risiken mit ökonomischem Eigenkapital in der Größenordnung von 15 – 25 % aus.[669] Zu diesem Zeitpunkt stellt der Ausschuss in Bezug auf das Risikomanagement dieser Risikoart allerdings fest[670]: „**Overall, the survey indicated that the quantification of operational risk is, for most institutions, at an early stage although progress is envisaged at many banks.** […] For most banks the tracking of risk indicators appears to be in its infancy, and a large number are not tracking indicators of any kind. Where indicators are tracked, the use to which they are put is often unclear for either risk management or economic capital allocation purposes.[…] Those banks working on an internal approach cited a lack of data as an impediment."

Andere Autoren wie Beeck und Kaiser berichten von Expertenschätzungen und ersten Messergebnissen Ende 1999, denen zufolge Operationelle Risiken einen Anteil von 20 – 40 % am Gesamtrisiko der Finanzinstitute ausmachen.[671] Ihren Angaben zufolge sind Kreditrisiken für die Hälfte des Gesamtrisikos zuständig, und der kleinere Restteil wären Marktpreisrisiken.

Eine erste empirisch basierte Annäherung, wie die unterschiedlichen Risikoarten im Bankensektor in Bezug auf die Größenordnungen zueinander stehen, liefern die begleitenden Arbeiten, die im Rahmen der Konsultationen zur Neuen Basler Eigenkapitalvereinbarung durchgeführt wurden. Bei der im Umfang bisher größten dritten Quantitative Impact Study (QIS3)[672], an der 365 Banken unterschiedlichster Größe aus mehr als 40 Ländern teilgenommen hatten, wurden weitgehend die bisherigen Annahmen des Basler Ausschusses für Bankenaufsicht bestätigt. Sowohl bei der geltenden als auch bei der Neuen Basler Eigenkapitalvereinbarung muss die Eigenkapitalquote, definiert als Anteil verfügbaren Eigenkapitals an einer definierten Messgröße von Risiken einer Bank, mindestens 8 % betragen. Allerdings hat sich der Nenner mit der Messgröße von Risiken erheblich verändert. Neben dem bisher berücksichtigten Kreditrisiko und Marktrisiko wird in Basel II das Operationelle Risiko explizit in die Berechnung mit aufgenommen.

Das Operationelle Risiko sollte bei den ersten Überlegungen im Rahmen von Basel II noch 20 % der gesamten Eigenkapitalanforderungen ausmachen. Die Kritik der Banken und die ersten Datenerhebungen durch die Quantitative Impact Study führten jedoch im Verlauf der Konsultationen in den letzten zwei Jahren zu einer Absenkung auf 12 %. Das führt zu einem Anteil von 0,96 % des verfügbaren Eigenkapitals an den berücksichtigten Gesamtrisiken.

5.3.2.2.2 Die quantitative Erfassung Operationeller Risiken in Basel II

Banken haben in Basel II, ähnlich wie bei der Kreditrisikoberechnung, auch bei der Berechnung Operationeller Risiken die Möglichkeit, aus drei verschiedenen Ansätzen zu wählen, die sich im Komplexitätsgrad bei der Datenerfassung und –aufbereitung erheblich unterscheiden. Die sogenannten fortgeschrittenen Ansätze verlangen erhebliche Anstrengungen bei den Banken, für die Erhebung und Aufbereitung der Daten. Anreiz, diese Ansätze zu verwenden, sollen niedrigere Eigenkapitalanforderungen sein; im Fall des Operationellen Risikos erklärt sich der Ausschuss für Bankenaufsicht sogar bereit weitestgehend eigene Ansätze der Banken zunächst zuzulassen. Erklärtes Ziel der Aufsicht ist es, in diesem sich stark entwickelnden

[669] Vgl. BIZ (2001c), S. 18, Annex 1.
[670] BIZ (2001c), S. 18. Fettdruck durch BIZ.
[671] Vgl. Beeck (2000), S. 650.
[672] BIZ (2003f), S. 2. Eigentlich sind es mit QIS2,5 bereits 4 Erhebungen.

Umfeld zunächst methodisch und in der Qualität der Datenerhebung mit der Entwicklung Schritt zu halten.[673] Ein weiterer Anreiz, die fortgeschrittenen Ansätze zu implementieren, ist die Möglichkeit, Versicherungen, die Schadensfälle aus Operationellen Risiken abdecken, zu berücksichtigen. Dadurch kann das Operationelle Risiko, das mit Eigenkapital unterlegt werden muss, um bis zu 20 Prozentpunkte gesenkt werden.

Ein grundsätzliches Problem für die Kalibrierung jeglicher Ansätze zur Quantifizierung Operationeller Risiken liegt in der (noch nicht) vorhandenen standardisierten Datenmenge. Die Schwierigkeiten beginnen mit einer über alle Institute gleichlautenden Kategorisierung, die keineswegs selbstverständlich ist, wie in Abschnitt 5.3.2.1 deutlich gemacht wurde.

Gleichwohl ist mit der „Loss Data Collection Exercise for Operational Risk" (LDCE), die im Rahmen der QIS3 durchgeführt wurde, ein weiterer Schritt in Richtung Aufbau eines konsistenten institutsübergreifenden Datenbestandes getan.[674] Von 89 im Jahr 2002 an der LDCE teilnehmenden Finanzinstituten wurden 47269 einzelne Schadensfälle berichtet. Zum Vergleich: Ende 2001 berichteten Stocker et al. über die Entwicklung eines Betriebsrisiko-controllings in der Bayrischen Landesbank; unter anderem wurde dort auf eine Schadensdatenbank mit 5.000 öffentlichen Fällen zurückgegriffen.[675] Bei der Erhebung, die von der BIZ für die Jahre 1998 – 2000 durchgeführt wurde, wurden lediglich 30 Banken gefunden, die in der Lage und bereit waren, die gewünschten Daten mit der entsprechenden Kategorisierung bereitzustellen.[676] Besonders auffällig die deutlich geringere Anzahl an gemeldeten Schadensfällen: In den drei Jahren von 1998 – 2000 wurden insgesamt 27371 Verlustfälle gemeldet. Im Mittel pro Bank sind dies 304 Fälle pro Jahr; bei der Erhebung 2002 war diese Zahl auf 531 gestiegen, eine Steigerungsrate von 74 %. Diese Entwicklung zeigt, dass die „Kultur" der Schadensaufdeckung, -meldung und -erfassung über alle Geschäftsbereiche der Finanzinstitute zunächst verändert und entwickelt werden muss.

Die gesamte Schadenshöhe im Bereich Operationeller Risiken (entdeckter und gemeldeter Fälle) betrug für die 89 Banken für das Berichtsjahr 2001 fast € 7,8 Mrd.[677] Werden nur die Schäden betrachtet, die über der für Basel II als berichtspflichtig eingestuften Höhe von € 10.000 liegen, sinkt die Zahl der Banken, die in ihrem Berichtswesen diese Ereignisse aussortieren können, auf 63 Banken. Diese 63 Banken erlitten 2001 Schadensfälle mit einem Wert von € 5,8 Mrd.[678] Im Vergleich: die 30 Banken der ersten Erhebung über die drei Jahre 1998–2000 meldeten Schadensfälle in der Größenordnung von € 2,6 Mrd.[679]

Die Wahl des entsprechenden Ansatzes, den das jeweilige Finanzinstitut verfolgt, entscheidet über den Erhebungsaufwand für Operationelle Risiken. Die einzelnen Ansätze zur Quantifizierung der Operationellen Risiken, Basisindikatoransatz, Standardansatz, Alternativer Standardansatz und Fortgeschrittene Messverfahren (Advanced Measurement Approaches (AMA)), die zunehmend höhere Ansprüche an das Risiko-Management der Finanzinstitute stellen, werden in den folgenden Unterpunkten dargestellt und kurz diskutiert. Der Basler Ausschuss für Bankenaufsicht rechnet bereits in naher Zukunft damit, dass die Fortgeschrittenen Messverfahren die gleiche Datenqualität und Aussagekraft besitzen werden wie die

[673] Vgl. BIZ (2003c), S. 20 f.
[674] Vgl. BIZ (2003f), S. 2 ff.
[675] Vgl. Stocker et al. (2001), S. 683.
[676] Vgl. BIZ (2002a), Table 3. Nur 20 % der gelieferten Daten waren vollkommen verständlich und zuordenbar im Sinne der Vorgaben der Risk Management Group des Baseler Auschusses (BIZ (2002a), S. 3 f.).
[677] BIZ (2003f), S. 10, Tabelle 6, Panel A. Allerdings fallen auch die Terrorschäden durch den Anschlag am 11.09.2001 in den Erhebungszeitraum. Ein Vergleich mit Vor- oder Folgejahren wird somit zusätzlich erschwert.
[678] BIZ (2003f), S. 10, Tabelle 6, Panel B.
[679] BIZ (2002a), S. 5.

etablierten Verfahren im Bereich Markt- und Kreditrisiko.[680] Die Fortgeschrittenen Messverfahren stellen die höchsten Ansprüche an das Management Operationeller Risiken.

5.3.2.2.3 Basisindikatoransatz

Der Basisindikatoransatz verzichtet zunächst auf komplexe Verfahren zum Management Operationeller Risiken. Gleichwohl wird dieser Ansatz von der Aufsicht akzeptiert, solange noch kein fortgeschrittenes Verfahren angewendet wurde. Ein Rückschritt zum jeweils einfacheren Verfahren, wenn einmal ein komplexerer Ansatz bei der Aufsicht gemeldet wurde, ist nur mit Zustimmung der Aufsicht zulässig; erfüllt jedoch ein Institut nicht die von der Aufsicht vorgegebenen Kriterien in dem jeweils angewendeten Ansatz, kann die Aufsicht nach eigenem Ermessen das nächsteinfachere Verfahren vorschreiben.[681]

Die BIZ versucht bereits in den einfachen Ansätzen, die Banken auf die Anforderungen der fortgeschrittenen Verfahren einzustimmen, und ermuntert sie ausdrücklich, diese zukünftig anzuwenden. Von international tätigen Banken und solchen, die ein hohes Risiko für Operationelle Risiken aufweisen, wird der Einsatz der fortgeschrittenen Ansätze erwartet.[682]

Die „Sound Practices for the Management and Supervision of Operational Risk“ mit den zehn „Best Practices“-Grundsätzen des Managements Operationeller Risiken sollten idealerweise bereits beim Basisindikatoransatz Anwendung finden.[683] Die Formulierung der BIZ geht an dieser Stelle noch von einer Freiwilligkeit auf Seiten der Institute aus bei der Anwendung der Grundsätze.

Der Basisindikatoransatz geht vom durchschnittlichen jährlichen Bruttoertrag der Bank in den vorangegangenen drei Jahren aus. α für Bank j im Jahr t berechnet sich als[684]:

Formel (1) $$\alpha_{j,t} = \frac{0{,}12 * MRC_{j,t}}{GI_{j,t}}$$

mit

$MRC_{j,t}$: regulatorische Eigenmittel der Bank j im Jahr t (8 % Eigenkapitalunterlegung (übernommen aus Basel I))

$GI_{j,t}$: Bruttoeinkommen der Bank j im Jahr t

Der Faktor 0,12 ist der Anteil regulatorischen Eigenkapitals an den gesamten regulatorischen Eigenmitteln, der bei Basel II als empirisch erwiesen gilt.[685] In den ersten empirischen Berechnungen ist der Basler Ausschuss für Bankenaufsicht noch auf einen Wert für α zwischen 0,17 und 0,20 gekommen.[686] Der Basler Ausschuss für Bankenaufsicht hat im dritten Konsultationspapier nach erneuten Berechnungen den Risikofaktor α mit 0,15 angegeben. Wird der Bruttoertrag mit dem Risikofaktor multipliziert, resultiert daraus gemäß Formel (2) die notwendige Eigenkapitalunterlegung nach Basel II für Operationelle Risiken.[687]

---

[680] Vgl. BIZ (2003c), S. 10, Ziffer 41 f.
[681] Vgl. BIZ (2003d), S. 120.
[682] Vgl. BIZ (2003d), S. 120.
[683] Vgl. BIZ (2003c), S. 11.
[684] BIZ (2001i), S. 27.
[685] Vgl. BIZ (2001i), S. 25 f.
[686] Vgl. BIZ (2001i), S. 28.
[687] Vgl. BIZ (2003c), S 11.

Formel (2) $K_{BIA} = GI * \alpha$

mit

K_{BIA}: Eigenkapitalunterlegung für Operationelles Risiko bei Basisindikatoransatz

GI: durchschnittlicher Jahresbruttoertrag[688] gerechnet über die letzten drei Jahre

A: Risikofaktor für Operationelles Risiko, von Aufsicht festgelegt

Der Basisindikatoransatz dient zunächst einer Quantifizierung der aufsichtlichen Anforderung an die Eigenkapitalunterlegung Operationeller Risiken. Eine Steuerungswirkung im Sinne eines Managements Operationeller Risiken kann kaum erzielt werden.

Es kann erwartet werden, dass der Basisindikatoransatz in einer Übergangsphase zu Basel II verbreitet bei kleineren und spezialisierten Instituten Anwendung findet. Erfüllen sich die sehr positiven Erwartungen des Basler Ausschusses für Bankenaufsicht in Hinblick auf eine immer bessere Datenlage und ein risikosensitiveres Management Operationeller Risiken, kann in den nächsten Jahren mit einem abnehmenden Einsatz dieses simplifizierten Ansatzes gerechnet werden. Dies gilt umso mehr, je wirksamer sich die finanziellen Anreizstrukturen und eventuell resultierende Wettbewerbsvorteile für einzelne Finanzinstitute erweisen. Gibt es an dieser Stelle messbare Resultate, wird es institutsübergreifend zum Einsatz ähnlicher fortgeschrittener Ansätze kommen.

5.3.2.2.4 Standardansatz

Der Standardansatz ist aufwändiger in der Anwendung für die Finanzinstitute. Bei seiner Anwendung müssen die Institute gemäß vorgegebenen Geschäftsbereichen (die acht Business lines (Level 1) in Tabelle 9) wiederum als Grobindikator den Bruttoertrag jedes Bereichs ermitteln. Zusätzlich gibt Basel II einige qualitative Erwartungen an das Risikomanagement der Banken vor, die für die Erlaubnis der Anwendung des Standardansatzes vorausgesetzt werden. Die Aufsicht behält sich eine einjährige Testphase vor, bei der sie einen Eindruck von der Qualität der bankinternen Risikomanagementstrukturen erhält, bevor die Finanzinstitute den Standardansatz anwenden dürfen.[689] Diese Einschränkung gilt für alle weiterführenden Verfahren außer dem Basisindikatoransatz.

Im Wesentlichen sind diese qualitativen Anforderungen der Aufsicht an die Finanzinstitute ein Spiegelbild der zehn Grundsätze der „Sound Practices for the Management and Supervision of Operational Risk“[690]. Das bedeutet, die Funktion des Managements Operationeller Risiken muss auf oberster Führungsebene verantwortet werden, die Prozesse müssen durch das gesamte Institut definiert sein, ein wirksames Berichts- und Dokumentationswesen bis auf Vorstandsebene muss ebenso existieren wie Anreize in den einzelnen Geschäftsbereichen, die Maßnahmen zur Beherrschung Operationeller Risiken umzusetzen. Dazu kommt die Pflicht, das gesamte Operational Risk Management regelmäßig unabhängig zu bewerten und zu überprüfen. Für die Anwendung des Standardansatzes ist die Umsetzung dieser Anforderungen notwendig, ansonsten kann die Aufsicht die Zulassung verweigern. Erst an letzter Stelle der Nennungen findet sich ein Hinweis darauf, dass die Banken, die den Standardansatz anwenden wollen, in der Lage sein müssen, die Bruttoerträge gemäß den acht von Basel II vorgegebenen Geschäftsbereichen auszuweisen.[691] Allein diese Fähigkeit entscheidet über die Anwendbarkeit des Ansatzes.

---

[688] Zur genauen Definition des Bruttoertrags vgl. BIZ (2003d), S. 121, Ziffer 613.
[689] BIZ (2003d), S. 123.
[690] Vgl. BIZ (2003d) und BIZ (2003a).
[691] BIZ (2003d), S. 125, Ziffer 625.

Ausgangspunkt der Überlegungen beim Standardansatz ist, dass verschiedene Geschäftsbereiche in unterschiedlichem Maße Operationellen Risiken ausgesetzt sind. Dieser Risikoexponiertheit wird in Analogie zum Basisindikatoransatz mit einem Faktor β Rechnung getragen, der für die einzelnen Bereiche unterschiedlich ausfällt und von der Aufsicht bestimmt wird.

Die notwendige Eigenkapitalunterlegung resultiert dann aus der Anwendung von Formel (3):[692]

Formel (3) $$K_{TSA} = \sum_{i=1}^{8} (GI_i * \beta_i)$$

mit

K_{TSA}: Eigenkapitalunterlegung für Operationelles Risiko bei Standardansatz
GI_i: durchschnittlicher Jahresbruttoertrag der einzelnen Bereiche, gerechnet über die letzten drei Jahre, (i = 1...8)
β_i: Risikofaktor für Operationelles Risiko, von Aufsicht für jeden Bereich i einzeln festgelegt, (i = 1...8)

Die jeweiligen Faktoren $\beta_{j,i}$ der Banken j werden analog zu α von der Aufsicht auf Grundlage empirischer Daten im Geschäftsbereich i berechnet:[693]

Formel (4) $$\beta_{j,i} = \frac{(0{,}12 * MRC_j * OpRiskShare_{j,i})}{GI_{j,i}}$$

mit

MRC_j: regulatorische Eigenmittel der Bank j (8 % Eigenkapitalunterlegung (übernommen aus Basel I))
$GI_{j,i}$: Bruttoeinkommen der Bank j im Geschäftsbereich i
$OpRiskShare_{j,i}$: Anteil ökonomischen Kapitals für Operationelle Risiken der Bank j im Geschäftsbereich i

Die Aufsicht hat auf Grundlage von QIS3 die Werte der Faktoren β_i, (i = 1...8), wie in Tabelle 12 festgelegt.

Geschäftsbereich$_i$		**Faktor β_i**
Corporate finance (Unternehmensfinanzierung)	(β_1)	18 %
Trading and sales (Handel)	(β_2)	18 %
Retail banking (Privatkundengeschäft)	(β_3)	12 %
Commercial banking (Commercial Banking)	(β_4)	15 %
Payment and settlement (Zahlungsverkehr)	(β_5)	18 %
Agency services (Agency und Depotgeschäft)	(β_6)	15 %
Asset management (Vermögensverwaltung)	(β_7)	12 %
Retail brokerage (Wertpapierprovisionsgeschäft)	(β_8)	12 %

Tabelle 12: Risikofaktoren β_i beim Standardansatz für die geforderte Eigenmittelunterlegung Operationeller Risikrn einzelner Geschäftsbereiche[694]

[692] BIZ (2003d), S. 122 f.
[693] BIZ (2001i), S. 28 f.
[694] BIZ (2003d), S. 123.

Gegenüber dem Basisindikatoransatz, der den Bruttoertrag mit $\alpha = 0{,}15$ multipliziert, existiert für die Finanzinstitute lediglich dann ein finanzieller Anreiz, den Standardansatz zu verwenden, wenn gilt:

$K_{TSA} < K_{BIA}$

Dies gilt genau dann, wenn gilt:

$$(GI_1 + GI_2 + GI_5)* 0{,}18 + (GI_3 + GI_7 + GI_8)*0{,}12 < (GI_1 + GI_2 + GI_3 + GI_5 + GI_7 + GI_8)*0{,}15$$

Diese Bedingung kann bei Finanzinstituten erfüllt sein, die im Privatkundengeschäft, der Vermögensverwaltung und/oder dem Wertpapierprovisionsgeschäft besonders aktiv sind im Vergleich zu den anderen Geschäftsbereichen, die mit einem β von 0,18 hoch gewichtet werden.

Es bleibt abzuwarten, ob der finanzielle Anreiz, der sich aus der Differenz von K_{TSA} und K_{BIA} ergibt, tatsächlich ausreicht, um vor allem kleinere Institute der Gruppe 2 zu motivieren, die anspruchsvollen „Sound Practices" institutsweit umzusetzen – sofern nicht ein legislativer Anreiz diesen Aspekt obsolet macht.

5.3.2.2.5 Alternativer Standardansatz

Die Schwierigkeiten einer genauen Quantifizierung der Operationellen Risiken wurden bei QIS3 auch an anderer Stelle deutlich. Im Mittelwert erreichen die Banken zwar eine Eigenkapitalanforderung von 12 %, nur ist die Varianz aufgrund der unterschiedlichen Geschäftsstruktur der betroffenen Banken so erheblich, dass sich der Basler Ausschuss für Bankenaufsicht entschlossen hat, einen alternativen Standardansatz zuzulassen, der insbesondere bei Abweichungen nach oben mit der Vermeidung von Doppelzählungen die vermutete zu hohe Belastung der Banken reduziert. Der alternative Ansatz kann im Einvernehmen mit den nationalen Aufsichtsinstanzen verwendet werden.[695] Hintergrund ist ein Problem, das erst mithilfe der empirischen Daten der QIS3 offensichtlich wurde. Es kann bei Verwendung des Standard-Ansatzes zu einer zu hohen Eigenmittelunterlegung für Operationelle Risiken kommen, wenn Finanzinstitute im klassischen Bankgeschäft zu hohe Margen auf einzelne Produkte verlangen (können), beispielsweise für bestimmte Risiken bei der Kreditvergabe.

Der alternative Ansatz versucht diese Schwierigkeiten zu umgehen, indem für den Privatkunden- und Commercial Bankingbereich ein zusätzlicher Faktor m eingeführt wird, der analog zu den Risikofaktoren α und β von der Aufsicht festgelegt wird. Anstelle des Bruttoertrags wird dieser Faktor m mit dem in diesem Bereich vergebenen Kreditvolumen multipliziert. Das notwendige Eigenkapital für Operationelle Risiken berechnet sich wie in Formel (5) angegeben.

Formel (5) $$K_{TASA} = K_{RB} + K_{CB} + \sum_{k=1}^{6} TSA_k$$

mit

$K_{RB} = \beta_3 * m * LA_{RB:}$ Eigenkapitalanforderung für Privatkundenbereich (RB)

$K_{CB} = \beta_4 * m * LA_{CB:}$ Eigenkapitalanforderung für Geschäftskundenbereich (CB)

[695] Vgl. BIZ (2003c), S. 20 f, BIZ (2003d), S. 122.

$K_{TSA,\,k} = \sum_{k=1}^{6} GI_k * \beta_k$,mit k = 1..6: Eigenkapitalanforderung für die restlichen sechs Geschäftsbereiche

mit

K_{TASA}: Eigenkapitalunterlegung für Operationelles Risiko bei Alternativem Standardansatz

GI_i: durchschnittlicher Jahresbruttoertrag der einzelnen Bereiche gerechnet über die letzten drei Jahre (i = 1..6)

β_i: Risikofaktor für Operationelles Risiko, von Aufsicht für jeden Bereich i = 1...8 einzeln festgelegt; gleiche Werte wie bei Standardansatz

m: Kalibrierungsfaktor, von Aufsicht mit 0.035 vorgegeben

LA_{RB}: Summe vergebener Kredite im Privatkundenbereich (gemittelt über die drei letzten Jahre)

LA_{CB}: Summe vergebener Kredite im Bereich Commercial Banking (gemittelt über die drei letzten Jahre)

Vereinfachend können Banken die Bereiche Privatkunden und Commercial Banking aggregieren, mit der Folge, dass statt acht noch sieben Geschäftsbereiche betrachtet werden. Allerdings wird β dann auf 0,15 angehoben, eine geringfügige Verschlechterung aus Sicht der Bank, die sonst im Privatkundengeschäft mit 0,12 rechnen könnte. Ferner können Banken die anderen sechs Geschäftsbereiche bei Erhebungsproblemen zusammenfassen und einen Faktor β von 0,18 anwenden.[696] Auch in diesem Fall verschlechtert sich die Rechnung für die Bank, da 0,18 die Obergrenze der βs im Standardansatz darstellt, die zwischen 0,12 und 0,18 liegen.

Analog zur Berechnung beim Standardansatz ist der Einsatz des Alternativen Standardansatzes betriebswirtschaftlich nur dann lohnend, wenn gilt:

$K_{TASA} < K_{TSA} < K_{BIA}$

Es gibt bei den von der Aufsicht vorgeschlagenen Faktoren (Stand Juni 2003) keinen Anreiz für die Wahl des für beide Bereichsgruppen aggregierten Alternativen Standardansatzes, da immer gilt:

$K_{TASAaggregiert} > K_{BIA}$

Weder der Standardansatz noch der Alternative Standardansatz erfordern auf der quantitativen Seite ein dezidiertes Risikomanagement für Operationelle Risiken. Das Operationelle Risiko und die dazu notwendige Eigenmittelunterlegung wird über Geschäftskennzahlen wie den Bruttoertrag für die gesamte Bank oder einzelne Geschäftsbereiche oder die Summe vergebener Kredite abgeleitet. Ziel ist es, eine mit Basel II notwendige Eigenmittelunterlegung für Operationelle Risiken errechnen zu können.

Allerdings müssen die Finanzinstitute, ein den „Sound Practices of the Management and Supervision of Operational Risk“ angepasstes Risikomanagement etablieren. Bestätigen sich die empirischen Ergebnisse der QIS3, die deutliche Cluster in Bezug auf Höhe und Anzahl der Schadensfälle im Bereich Privatkundengeschäft und Commercial Banking ergeben, kann es sich in Zukunft auch für kleinere Institute betriebswirtschaftlich rechnen, mindestens in diesen Bereichen Risikomanagementstrukturen aufzubauen. Dies gilt umso mehr, je besser solche Strukturen mit softwarebasierten Werkzeugen aufgebaut und unterstützt werden

[696] Vgl. BIZ (2003d), S. 122.

können.[697] Die Aufsicht lässt in Basel II einen Weg offen, bei dem Institute unter bestimmten Voraussetzungen teilweise die fortgeschrittenen Ansätze verwenden können, und somit von eventuellen Reduktionen beim notwendigen Eigenkapital profitieren können.[698]

Weder Basisindikatoransatz noch Standardansatz oder Alternativer Standardansatz verwenden explizit die Ergebnisse der Datenerhebungen im Bereich Operationeller Risiken. Ansonsten würde vermutlich die Varianz der Risikofaktoren β_i eine größere sein. Die Qualität der Daten kann jedoch nach Angaben der BIZ zum gegenwärtigen Zeitpunkt zur Kalibrierung dieser Modelle nicht dienen, da die Zweifel der Aufsicht an der Validität und Repräsentativität der Daten groß sind.[699]

5.3.2.2.6 Fortgeschrittene Messverfahren

Die anspruchvollsten Verfahren zur Berechnung wie zum Management Operationeller Risiken finden sich bei den Fortgeschrittenen Messverfahren (Advanced Measurement Approaches (AMA)). Auch bei den AMA finden sich aufsichtliche quantitative und qualitative Vorgaben, die von den Instituten erfüllt sein müssen, bevor die Zulassung erfolgt.[700] Mehr als die Hälfte der Seiten in der Neuen Basler Eigenkapitalvereinbarung, die sich mit den möglichen Verfahren zur Quantifizierung Operationeller Risiken beschäftigen, sind den Anforderungen an die AMA gewidmet.[701]

Bei den AMA erfolgt die Freigabe nach Einschätzung durch die Aufsicht, die den Eindruck gewinnen muss, der Ansatz wäre „credible and appropriate“ und das interne Messverfahren für Operationelle Risiken „must reasonably estimate unexpected losses based on the combined use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors.“[702]

Diese Anforderungen scheinen sehr subjektiv. Einerseits ist der Aufsicht bewusst, dass die empirischen Daten, die ihr vorliegen, aller Voraussicht nach nicht repräsentativ sind, andererseits sind die statistischen Verfahren nur dann in der Lage „reasonably“ unerwartete Verluste zu schätzen, wenn genau diese Datenreihen zuverlässig vorliegen. Es bleibt auch an dieser Stelle abzuwarten, wie diese Passagen von der Aufsicht in der täglichen Praxis umgesetzt werden. Zunächst wird von der Aufsicht gefordert, die verschiedenen Ansätze vor der Anerkennung parallel zu fahren; somit liegen der Aufsicht Vergleichswerte aus anderen Verfahren vor deren eigentlicher Genehmigung vor.

Die qualitativen Anforderungen orientieren sich wie bereits beim Standardansatz sehr stark an den zehn Grundsätzen der „Sound Practices“. Zusätzlich wird die Notwendigkeit von Prüfprozessen betont, die sicherstellen, dass die internen Bewertungsverfahren für Operationelle Risiken zufriedenstellend funktionieren und dass die internen Prozesse so aufgestellt sind, dass Aufsicht und Auditoren jederzeit einfach Zugang zu relevanten Daten und Verfahren haben.[703]

---

[697] Vgl. z. B. Interexa (2002).
[698] Vgl. BIZ (2003d), S. 130. Allerdings erwartet die Aufsicht im nächsten Schritt einen erkennbaren institutsweiten Übergang zu den fortgeschrittenen Ansätzen.
[699] Vgl. BIZ (2002a), S. 2.
[700] Vgl. BIZ (2003d), S. 123 ff.
[701] Operational Risk wird in BIZ (2003d) auf den Seiten 120 – 130 behandelt. Auf den Seiten 123 –130 geht es vornehmlich um AMA.
[702] BIZ (2003d), S. 123 f., Ziffer 622.
[703] Vgl. BIZ (2003d), S. 125 f.

Generelle Anwendung bei den AMA finden die Überlegungen und Anforderungen der Aufsicht, die aus Teil 2 „Supervisory Guidance for a Comprehensive Operational Risk Management Programme“ der „Sound Practices“ hervorgehen.[704] Auch wenn einzelne Überlegungen in Teil 2 nicht mehr gelten, beispielsweise wurde bei der Datensammlung der Schadensfälle auf die Quantifizierung anhand der Auswirkungen auf die Gewinn- und Verlustrechnung (sogenannter „loss effect types“) verzichtet[705], sind die meisten Anregungen und Ansätze in diesem Teil noch immer aktuell und finden sich in den Argumentationslinien der Folgeaufsätze der BIZ.

Die Dynamik bei der Modellierung Operationeller Risiken wird von der Aufsicht anerkannt. Dementsprechend vage fallen die quantitativen Vorgaben aus. Es wird in erster Linie erwartet, dass die Finanzinstitute mit ihren Methoden bekannte Möglichkeiten aus dem Management anderer Risiken abdecken, z. B. die Sicherstellung eines 99,9 % Konfidenzintervalls für das Eintreten unerwarteter Verluste aus Operationellen Risiken.[706] Bei aller Flexibilität ist die Aufsicht entschlossen, am Ende des ersten Jahres der erfolgten Quantifizierung durch AMA, d.h. Ende 2006, die Modelle aller Finanzinstitute zu überprüfen und gegebenenfalls Änderungen bei den AMA durchzusetzen.

Bei den detaillierten quantitativen Vorgaben fallen zwei besonders auf, während die anderen wiederum lediglich betonen, die Maßnahmen sollten mit den „Sound Practices“ konform sein. Zum einen wird von den Instituten erwartet, das regulatorische Eigenkapital als Summe aus erwarteten und und unerwarteten Verlusten darzustellen. Die eigentlich im Risikomanagement unübliche Berücksichtigung erwarteter Verluste kann nur dann aufgehoben werden, wenn die Bank nachweisen kann, dass sie die erwarteten Verluste in der Gestaltung ihrer Margen und Risikovorsorge adäquat berücksichtigt. Eine Forderung, die angesichts der (noch) nicht so weit entwickelten Systeme zunächst unrealistisch sein dürfte. Zum anderen wird die Problematik der Korrelation Operationeller Risiken berücksichtigt. Gelingt es den Instituten, die Verwendung geeigneter Verfahren zur Ermittlung der Korrelationen nachzuweisen, können sie diese verwenden. Dies hätte zur Folge, dass die reine Summierung der Operationellen Risiken um die Korrelationen bereinigt werden kann (ein Vorgang der bei Value-at-Risk-Ansätzen im Bereich Markt- und Kreditrisiken zu erheblichen Reduktionen führen kann) und die notwendige Eigenmittelunterlegung sinkt.[707]

Die weiteren Anforderungen an die interne Datenerhebung resultieren aus den Erfahrungen der BIZ mit den QIS. So müssen bestimmte Klassifikationsschemata eingehalten werden, Mindestwerte bei der Erfassung von Schadensereignissen institutsweit greifen und zusätzliche Informationen zu Schadensfällen, wie beispielsweise nach Schäden erfolgte Versicherungszahlungen, dokumentiert werden. Darüber hinaus sollten die Institute die Hintergründe und Ursachen bestimmter Schadensfälle im Verhältnis zur Schadenssumme ausführlich dokumentieren.[708]

Externe Daten, das heißt der Rückgriff auf spezialisierte Datenbanken, sind aus Sicht der Aufsicht insbesondere dann erforderlich, wenn „low frequency-high impact“-Schäden auftreten können, die für statistische Aufbereitungen innerhalb eines Instituts nicht in ausreichender Zahl dokumentiert sind. Es wird von den Banken erwartet, dass sie geeignete Indikatoren definieren, um die Relevanz externer Schadensfälle für die eigene Institution

[704] Vgl. BIZ (2001l), S. 12 ff.
[705] Vgl. BIZ (2001l), S. 14 und BIZ (2002b), S.2.
[706] Vgl. BIZ (2003d), S. 126 f.
[707] Vgl. BIZ (2003d), S. 126.
[708] Vgl. BIZ (2002a), BIZ (2002i), S. 41 f. und BIZ (2003d), S. 127 f.

einschätzen zu können. Ergänzt werden sollte diese Einschätzung durch Expertenbefragungen im Rahmen von Szenarioanalysen. Um der Problematik vergangenheitsbasierter Schadensfälle in einem sich dynamisch entwickelnden Umfeld zu entgehen, fordert Basel II weiter die Anwendung vorausschauender Methoden, beispielsweise die Entwicklung von Risikoindikatoren, die diese Dynamik berücksichtigen.[709]

Im Rahmen der Konsultationen zur Unterlegung Operationeller Risiken mit Eigenmitteln wurden in einem frühen Stadium die möglichen Versicherungen gegen diese Risiken diskutiert. Basel II lässt erst ab den AMA zu, dass Unternehmen ihre Versicherungen berücksichtigen. Dies beruht einerseits auf der Annahme, dass nur das versichert werden kann, was durch entsprechende Methoden annähernd bekannt ist, andererseits soll an dieser Stelle auch ein Anreiz geschaffen werden, die AMA einzuführen. Die genauen Konditionen werden in der dritten Konsultationsphase noch diskutiert[710], sicher ist, dass die Institute maximal 20 % ihrer notwendigen Eigenmittelquote für Operationelle Risiken über existierende Versicherungen senken können. Explizit müssen versicherungstypische Risiken, beispielsweise Kündigung nach Schadensfall oder Verweigerung/Verzögerung der Zahlung im Schadensfall bei der Kalkulation berücksichtigt werden.[711]

5.3.2.2.7 Modellansätze zur Quantifizierung Operationeller Risiken, die laut Basel II bei den Fortgeschrittenen Verfahren verwendet werden können

Allen Ansätzen gemein ist der notwendige Aufbau von Datenbanken, internen zunächst, aber auch externen zur späteren Validierung. Die Vorgaben der BIZ zur Klassifikation der Geschäftsbereiche und Verlustarten wie sie in Tabelle 9 und Tabelle 10 zum Ausdruck kommen, erweisen sich als wegweisend für den Aufbau von institutsübergreifenden Verlustdatenbanken. Erst eine systematische Erfassung, die institutsübergreifend die gleiche Klassifikation verwendet, kann im Bereich Operationeller Risiken, die sich durch andere statistische Gesetzmäßigkeiten auszeichnen als die Markt- und Kreditrisiken, ein quantitativ fundiertes Risikomanagement ermöglichen.

Der Basler Ausschuss für Bankenaufsicht teilt die Verfahren, mit denen aus seiner Sicht in Zukunft bei den AMA gearbeitet werden kann, in drei Kategorien: „Internal Measurement Approaches“ (IMA), „Loss Distribution Approaches“ (LDA) und Scorecard-Ansätze.[712] Der Ausschuss überlässt den Finanzinstituten bei der Wahl der Ansätze aber auch bei Neuentwicklungen im Wesentlichen die Entscheidung. Einzige Bedingung für die Anerkennung durch die Aufsicht ist ein geeigneter Nachweis über die Tauglichkeit des gewählten Ansatzes. Die Kombination einzelner Verfahren ist zulässig und im Fall der Anwendung von Scorecard-Ansätzen erscheint sie faktisch notwendig, da ansonsten die quantitative aufsichtliche Überprüfung nicht möglich erscheint.

Der Basler Ausschuss für Bankenaufsicht ist sich bewusst, dass alle Verfahren zumindest im Hinblick auf Operationelle Risiken eine kontinuierliche Entwicklung verlaufen und bislang noch kein Industriestandard, der übernommen werden könnte, in Sicht ist. Darin liegt für die bei den QIS und in den Konsultationen zu Basel II involvierten Finanzinstitute eine klare Möglichkeit, gestaltend in aufsichtliche Anforderungen an den Umgang mit Operationellen Risiken einzugreifen.

[709] Vgl. BIZ (2003d), S. 128 f.
[710] Vgl. BIZ (2003d), S. 129 FN 94.
[711] Vgl. BIZ (2003d), S. 130.
[712] Vgl. BIZ (2001i), S. 33 ff.

5.3.2.2.7.1 Internal Measurement Approaches

Bei den Internen Bemessungsansätzen (IMA)[713] ist die Grundlage der Berechnungen der regulatorischen Eigenmittel für Operationelle Risiken die Schätzung der erwarteten Verluste. Dabei wird von einer stabilen Verteilungsfunktion der Risiken ausgegangen, d.h. das Verhältnis erwarteter zu unerwarteten Verlusten bleibt annähernd konstant.

Für jede Verlustkategorie innerhalb eines Geschäftsbereichs kann eine Verlustverteilung und auf Grundlage der voraussichtlichen Schadenshöhen der Erwartungswert für erwartete Schäden durch Operationeller Risiken berechnet werden, basierend auf internen wie externen Datensätzen.

Die Kennzahlen der IMA sind nach BIZ gerechnet auf eine Periode t (in der Regel t = 1 Jahr):

$PE_{i,n}$: Wahrscheinlichkeit, dass ein Schadensereignistyp n in Geschäftsbereich i auftritt

$LGE_{i,n}$: Durchschnittliche monetarisierte Schadenshöhe eines Schadensereignistyps n in Geschäftsbereich i

EI_i : Aktivitätsparameter für bestimmte Geschäftsbereiche i in Relation zu anderen Geschäftsbereichen (trägt der Spezialisierung einzelner Institute Rechnung)

EL_i : Erwartete Verlusthöhe in Abhängigkeit vom Aktivitätsniveau des jeweiligen Geschäftsbereichs i (d.h. im Verhältnis zum erzielten Umsatz oder anderen Kenngrößen)

Somit errechnen sich die regulatorischen Eigenmittel $K_{i,n}$ für Operationelle Risiken für jede Kombination von Geschäftsbereichen i mit Schadensereignisstyp n:

Formel (6) $K_{i,n} = \gamma_{i,n} * EI_{i,n} * PE_{i,n} * LGE_{i,n} = \gamma_{i,n} * EL_{i,n}$

Die regulatorische Eigenmittelunterlegung für Operationelle Risiken ergibt sich unter der empirisch bislang unbestätigten Annahme fehlender Korrelationen zwischen einzelnen Schadensfällen als Summe der $K_{i,n}$.

$\gamma_{i,n}$ ist der für jede Kombination Geschäftsbereich/Schadensfall von der Aufsicht festzulegende oder zu genehmigende Faktor, der angibt, wie erwartete Verlusthöhen in Eigenkapital umzurechnen sind. Nach Ansicht der BIZ können die $\gamma_{i,n}$ auf Grundlage bankinterner Datensätze oder gepoolter Datensätze berechnet werden.

Der Ausschuss schlägt ein weiteres Verfahren vor, den „Risk Profile Index“ (RPI), mit dessen Hilfe unterschiedliche Formen der Verteilungsfunktionen der Schadensereignisse zwischen individuellem Finanzinstitut und dem Branchendurchschnitt bei der Bestimmung der $\gamma_{i,n}$ aufgefangen werden sollen.[714] Statt einer Normalverteilung werden gerade für die „low frequency – high impact“-Risiken rechtsschiefe Verteilungen erwartet, die von Institut zu Institut jedoch unterschiedlich akzentuiert ausfallen können. Der Risk Profile Index ergibt sich als Verhältnis der unerwarteten zu den erwarteten Verlusten und ist annahmegemäß eins für die branchenweite Gesamtverteilung. Das benötigte regulatorische Eigenkapital K errechnet sich mit dem RPI-Korrekturfaktor als:

[713] BIZ (2001i), S. 33 f.
[714] Vgl. BIZ (2001c), S. 24 f.

Formel (7) $$K = \sum_{i=1}^{l}\sum_{n=1}^{m} \Sigma i\, \Sigma n\, [\gamma_{i,n} * EI_{i,n} * PE_{i,n} * LGE_{i,n} * RPI_{i,n}]$$

Die Berechnungen der $RPI_{i,n}$, ebenso wie die Frage, ob dem Aufwand für diese Berechnungen ein entsprechender Nutzen gegenübersteht, oder ob alternative bessere Ansätze existieren, sind noch in den Anfängen der regulatorischen Überlegungen.

5.3.2.2.7.2 Loss Distribution Approaches

Die Loss Distribution Approaches[715] (LDA) beruhen auf der Schätzung der Verlustverteilung für jeden Verlusttyp in den einzelnen Geschäftsbereichen innerhalb eines bestimmten Beobachtungszeitraums – in der Regel ein Jahr. Die Schätzung bezieht sich dabei neben der Wahrscheinlichkeit für das Auftreten einzelner Schadensfälle jeweils noch auf die erwartete Schadenshöhe. Dabei müssen entsprechende Verteilungsannahmen getroffen werden. Die BIZ nennt beispielhaft eine Poisson-Verteilung für die Anzahl der Schadensfälle und eine Lognormal-Verteilung für die Schadenshöhe einzelner Ereignisse. Eine andere Möglichkeit wäre die empirische Ermittlung der Verteilungen beispielsweise per Monte Carlo Simulationen.

Sind die Verteilungen ermittelt oder angenommen, kann die regulatorische Eigenmittelunterlegung als Summe der „Operational-Value-at-Risk"- Schätzungen (OpVaR) für jeden Schadensfall in jeder Kategorie ermittelt werden; zumindest unter der Annahme unabhängiger Verlustereignisse, sonst müssen Korrekturfaktoren mittels Korrelationsmatrix berücksichtigt werden.

Die LDAs haben mehrere Vorteile gegenüber den IMAs: Die erwarteten Verluste werden direkt geschätzt und ergeben in ihrer Summe die notwendige Eigenkapitalunterlegung. Eine Abschätzung des Verhältnisses von erwarteten zu unerwarteten Verlusten und der dabei notwendigen einschränkenden Annahmen wie bei den IMAs nötig entfällt. Dadurch muss weder der Faktor γ noch ein Risk Profile Index geschätzt werden.

Ein weiterer Vorteil ist die mittlerweile etablierte oder absehbare Verwendung von VaR-Ansätzen im Bereich der Markt- und Kreditrisiken. Eine Integration der Operationellen Risiken in die Steuerungsinstrumente der Banken würde eine Gesamtbank-Risikosteuerung erheblich vereinfachen. Die Messung von Marktpreisrisiken ist bereits sehr gut eingeführt, die Datenlage verhältnismäßig unkritisch.

Bei den Ausfallrisiken sieht Buhr die Methoden als weitgehend ausgereift an, aber die endgültige Anwendung in der Praxis steht noch aus.[716] Allerdings ist von der Mehrzahl der Kreditinstitute nicht zuletzt aufgrund aufsichtlicher Vorgaben wie den MaK vorgesehen, diese Ansätze im operativen Geschäft einzusetzen. Ein Grund für eine zögerliche Anwendung ist die schwierige Datenlage. Die Zuordnung von Ausfallrisiken zu bestimmten Kreditrisiken leidet unter dem Problem, dass weder eine einheitliche Kategorisierung der Kreditnehmer noch eine systematische Erfassung der Kredite, der Risiken und der Ausfälle existiert haben und erst in den letzten Jahren die entsprechenden Daten erhoben werden.

Die Diskussion um die Bonitätsberücksichtigung bei der Vergabe von Krediten im Rahmen von Basel II bewirkt bereits im Vorfeld eine Ausweitung der VaR-Ansätze im Bereich

[715] BIZ (2001i), S. 34.
[716] Vgl. Buhr (2000), S. 202.

Kreditrisiko. Die verschiedenen Verfahren, die in der Praxis bereits angewendet werden, beispielsweise CreditMetrics, CreditRisk$^+$ oder CreditMonitor/PortfolioManager, unterscheiden sich teils erheblich in ihren Annahmen und gewichten die verwendeten Parameter unterschiedlich.[717] Bislang hat sich kein einheitliches Verfahren herauskristallisiert, jedes Verfahren hat Stärken und Schwächen und ist für bestimmte Belange geeigneter als für andere. Erschwerend wirkt sich aus, dass bei Markt- und Kreditrisiken unterschiedliche Zeithorizonte für die Bewertungsfragen berücksichtigt werden müssen. Rudolph und Johanning machen auf die unterschiedlichen Kulturen in den Finanzsystemen aufmerksam.[718] Im angelsächsischen Raum ist das Marktwertkonzept, das auf taggleiche Bewertungen der Positionen sowohl im Bereich Markt- als auch Kreditrisiken setzt, ungleich leichter durchzuführen als im deutschen Sprachraum, in dem aufgrund der Marktstruktur keine aussagefähigen Marktwerte für Kreditportefeuilles existieren. Erst wenn die Bewertungsfragen zufriedenstellend geklärt sind, erweist sich die Zuverlässigkeit eines integrierten Risikomanagements, das an einer VaR-Kennzahl entlang aufgebaut ist. Die mögliche Integration zusätzlicher OpVaR-Kennzahlen kompliziert diese Thematik.

Es gibt beim OpVaR-Ansatz einige methodische Probleme, die nicht vernachlässigbar erscheinen. Die Anforderungen an die zur Berechnung notwendigen Datenbanken sind relativ hoch, insbesondere was die Konsistenz und Anzahl der Daten angeht. Dazu müssten über die gesamte Bankorganisation die Verantwortlichen für das Einstellen von Schadensereignissen in Datenbanken, in einer einheitlichen Vorgehensweise geschult werden. Werden externe Datenbanken hinzugenommen, müsste die Vorgehensweise bei der Datenerhebung koordiniert werden. Die Schwierigkeiten dabei sind nicht zu unterschätzen, dies wurde unter anderem bei den Auswertungen der QIS deutlich.[719] Ferner ist methodisch die Frage noch ungeklärt, wie die Korrelationsmatrix, die zur Summenbildung der einzeln ermittelten OpVaR-Ergebnisse notwendig ist, aussehen könnte, und ob sie überhaupt zweifelsfrei errechnet werden kann.[720] Die Berücksichtigung von Korrelationen senkt prinzipiell den OpVaR. Buhr schlägt eine Methodik zur Ermittlung der Korrelationsmatrix vor, die darauf beruht, dass abgeschätzt wird, inwieweit Überlappungen zwischen einzelnen Schadensfällen existieren – ohne konkret darauf einzugehen, wie diese Überlappungen empirisch ermittelt werden. Er kommt zum Schluss seiner Ausführungen zu dem Ergebnis, dass aus Gründen der Praktikabilität zunächst auf die Berechnung von Korrelationsmatrizen verzichtet werden sollte und die vermutete resultierende Überzeichnung des OpVaR bei einfacher Summation der Einzel-OpVaR-Werte in Kauf genommen werden könne.[721] Simon hingegen bezweifelt die Transformationsmöglichkeit von VaR-Methoden aus dem Marktrisikobereich auf den Bereich Operationeller Risiken.[722] Rudolph und Johanning machen darauf aufmerksam, dass VaR-Kennzahlen als einzige Risikokennzahl nicht ausreichen, sondern um Sensitivitätsanalysen und Worst-Case-Szenarien ergänzt werden müssen.[723] Sie verweisen ferner darauf, dass der Vorteil einer scheinbar allgemeinverständlichen Risikokennzahl, die von Markt- über Kreditrisiken bis hin zu Operationellen Risiken alles in einer Zahl erfasst, bei VaR-Konzepten nicht darüber hinwegtäuschen darf, dass die unterschiedlichen Risiken in verschiedenen Kontexten wirken. Während Markt- und Kreditrisiken von der Bank im Rahmen der Risikotransformation bewusst eingegangen werden (sollten), sind Operationelle Risiken

[717] Vgl. ausführlich Rudolph (2000), S. 35 ff. und S. 45 ff.
[718] Rudolph (2000), S. 47.
[719] Vgl. BIZ (2002a), BIZ (2003f).
[720] Vgl. Hofmann (2002b), S. 81.
[721] Vgl. Buhr (2000), S. 205 f.
[722] Simon (2002), S. 147.
[723] Vgl. Rudolph (2000), S. 19 f.

lästige Begleiterscheinung und nach Möglichkeit zu vermeiden, zumindest wenn sie nicht wiederum selbst mit Risikoprämien versehen am Markt platziert werden können.

Ein weiteres Problem stellt die Tatsache dar, dass VaR-Verfahren theoretisch lediglich unter der Annahme verlässliche Schätzungen lieferen, dass die organisatorischen Rahmenbedingungen der Kreditinstitute im Beobachtungszeitraum konstant bleiben.[724] Diese Annahme ist unter zwei Aspekten fragwürdig. Zum einen wird bei Hinzunahme externer Daten ein breites Feld organisatorischer Regelungen betrachtet, zum anderen wird von der Aufsicht im Rahmen von Basel II und dem Supervisory Review Process gerade versucht, einen kontinuierlichen Wandel der organisatorischen Strukturen zur Bewältigung Operationeller Risiken einzuleiten. Burghof und Rudolph kritisieren bereits zu Beginn der Verwendung von Value at Risk Ansätzen 1996 die starke Gewichtung der Erfahrungen aus der Vergangenheit und die Notwendigkeit langer Zeitreihen bei den auf eine Risikomesszahl konzentrierten Verfahren.[725] Bielefeld geht noch einen Schritt weiter und stellt die Frage, ob überhaupt Werte aus der Vergangenheit als Grundlage für die Prognose der Zukunft verwendet werden können, bleibt Alternativen jedoch schuldig.[726]

Bislang ist der Basler Ausschuss für Bankenaufsicht – nicht zuletzt da kein allseits akzeptierter Ansatz existiert – offen für andere Verfahren, die auf Basis von OpVaR die notwendige Eigenkapitalunterlegung ermitteln.[727]

Vielversprechend erscheint der Ansatz der Extremwerttheorie, der lediglich das Verhalten der extremen Werte einer Datenreihe statistisch erfasst. Die Konzentration auf den Rand der Wahrscheinlichkeitsverteilung, in dem sich die für Operationelle Risiken typischen „low frequency – high impact"-Fälle befinden, kommt der Datenerfassungssituation deutlich näher als Annahmen über die Verteilungsfunktion selten eintretender Risiken. So wurden bei der QIS3 im Jahr 2002 bei der quantitativen Erhebung Operationeller Risiken in der Klasse mit Schäden über € 10.000 in 42 von 56 Kategorien lediglich 1 % der gemeldeten 47.000 Fälle in einem Beobachtungsjahr angegeben.[728] Hofmann beschreibt im theoretischen Ansatz die Möglichkeit, mit der „Peaks Over Threshold"-Methode (POT), bei der die Exzendenten über einem hohen Schwellenwert analysiert werden, Operationelle Risiken mit dem VaR-Ansatz zu quantifizieren.[729] Damit wird der Kritik an OpVaR-Konzepten begegnet, die diese Ansätze als generell ungeeignet für die Messung von „event risks" bezeichnen.[730] Borkovec und Klüppelberg machen am Beispiel von Finanzzeitreihen allerdings deutlich, dass für diese Methode ebenfalls eine gewisse Stichprobengröße notwendig wird.[731] Beispielsweise wird bei der von ihnen vorgestellten POT-Methode für stationäre Zeitreihen mit der Identifikation von Clustern gearbeitet, die mit einer Blocklänge von r = 20 relativ große Datenmengen benötigen. Zusätzlich ergibt sich das Problem, dass die verschiedenen POT-Methoden bei Quantilen in der Nähe von 1 – der Standardfall bei aufsichtlichen Vorgaben – stark unterschiedliche Aussagen liefern. Borkovec und Klüppelberg empfehlen daher immer die Anwendung mehrerer Verfahren;[732] aus Sicht der Anwendbarkeit der Methode in der Praxis ein Nachteil.

[724] Vgl. Hofmann (2002b), S. 81.
[725] Vgl. Burghof (1996), S. 143.
[726] Vgl. Bielefeld (2003), S. 29.
[727] Vgl. BIZ (2001i), S. 34.
[728] Vgl. BIZ (2003f), S. 6 f.
[729] Vgl. Hofmann (2002b), S. 67 ff.
[730] Vgl. Bielefeld (2003), S. 29.
[731] Vgl. Borkovec (2000).
[732] Vgl. Borkovec (2000), S. 241.

Die Evaluation einzelner bankinterner Methoden bleibt schwierig. Sie wird erst durch die aufwändige parallele Anwendung mindestens zweier verschiedener Verfahren möglich. Es existiert bislang kein allgemein anerkannter Ansatz, auf den sich die Aufsicht stützen könnte. Vermutlich wird es einen experimentellen Annäherungsprozess zwischen Aufsicht und Kreditinstituten geben. Dabei zeichnet sich eine grundsätzliche Bevorzugung der Value at Risk Verfahren ab, die obwohl komplex in der Anwendung, methodisch bereits bei den Markt- und Kreditrisiken mit Erfolg eingeführt sind.[733] Eine von allen Seiten gewünschte Gesamtrisikosteuerung rückt mit einem einheitlichen Ansatz, den die VaR-Methode prinzipiell bietet, deutlich näher.[734]

Für Bereiche, in denen bereits mit aufsichtlicher Genehmigung Bewertungsmodelle eingesetzt werden, um den Marktwert und die potenziellen Marktwertverluste zu berechnen, wird in den letzten Jahren vermehrt das Modellrisiko, die Fehlerrate der Risikoberechnung durch die Modellannahmen, untersucht. Rudolph vermutet, das dieses Risiko im Kreditrisikobereich höher liegt als im Marktrisikobereich und führt als Argument die Illiquidität der Kreditpositionen an.[735] Für den Bereich Operationeller Risiken gibt es zum gegenwärtigen Zeitpunkt aufgrund der fehlenden Vergleichsdaten keine empirischen Arbeiten. Operationelle Risiken sind größtenteils Risiken des internen Leistungsbereichs. Somit kann vermutet werden, dass bei fehlerhafter Modellierung das jeweilige Finanzinstitut zumindest flexibel auf die Ereignisse und mögliche Schäden reagieren kann, und dadurch größere Schäden bei einem funktionierenden Frühwarnsystem reduzieren oder vermeiden kann. Wird jedoch ein potenzieller Schaden im Modell als geringfügig betrachtet und stellt sich im realisierten und nicht mehr steuerbaren Schadensfall als „low frequency – high impact“ Schaden heraus, kann auch bei Bewertungsmodellen für Operationelle Risiken das Modellrisiko hoch sein.

5.3.2.2.7.3 Scorecard-Ansätze[736]

Die Ansätze, die mit Hilfe von Scorecards arbeiten, beruhen auf einem mehr in die Zukunft gerichteten Verständnis der Allokation von regulatorischem Eigenkapital für Operationelle Risiken. Ausgangspunkt ist eine vorab festgelegte Verteilung des regulatorischen Eigenkapitals auf die einzelnen Geschäftsbereiche. Ausgehend von einem angenommenen Risikoprofil und einer Einschätzung der Risikokontrollkapazität der einzelnen Bereiche wird mit Hilfe verschiedener, bankintern entwickelter Risikoindikatoren die Verteilung des Eigenkapitals auf die jeweiligen Bereiche dynamisch angepasst.

Die Scorecard-Ansätze haben den Vorteil, auf die tatsächliche aber auch lediglich angenommene Entwicklung der Risikomanagement-Qualität innerhalb eines Instituts zielgerichtet zu reagieren und die resultierende Veränderung der Eigenmittel sofort auf Geschäftsbereichsebene abzubilden. Diese Verfahren umgehen nicht die grundsätzliche Schwierigkeit, den Ausgangspunkt zu markieren, und dafür auf Vergangenheitsdaten und nicht nur auf die zukünftige Entwicklung angewiesen zu sein. Demzufolge müssen Scorecard-Ansätze, bevor sie von der Aufsicht zugelassen werden, ebenso wie IMAs und LDAs den Nachweis der Verwendung eines geeigneten Verfahrens zur Bestimmung der Ausgangsposition auf Grundlage historischer Daten erbringen.

Im laufenden Betrieb muss eine Kalibrierung und Validierung der Scorecard-Ansätze durch wiederholte Berechnungen auf Grundlage der Vergangenheitsdaten erfolgen. Vorteil der

[733] Vgl. u.a. Anders (2001), Buhr (2000), Brink van den (2002), Hofmann (2002b), Interexa (2002).
[734] Einen Vorschlag für eine solche Gesamtrisikosteuerung zeigt Buhr (2000) auf.
[735] Rudolph (2000), S. 24.
[736] BIZ (2001i), S. 34 f.

Verfahren ist die mögliche Einbringung qualitativer Elemente, beispielsweise durch die Konstruktion eines Risikoindex, der auf Experteneinschätzungen beruht. Bislang gibt es noch kein etabliertes Verfahren in diesem Segment, nicht zuletzt weil auch die vergleichenden Messverfahren in der Erprobung sind.

5.3.2.3 Risikoinstrumente und Maßnahmen zur Steuerung von Operationellen Risiken

Allgemeinen Systematisierungsansätzen folgend können drei Steuerungsebenen unterschieden werden. Die primäre Steuerungsebene versucht das Risiko durch Wissensmanagement und eine geänderte Gestaltung der Aufbau- und Ablauforganisation ursachenbezogen (ätiologisch) zu kontrollieren und zu beherrschen. Auf der sekundären und tertiären Ebene kommen wirkungsbezogene (palliative) Ansätze zum Tragen. Auf der sekundären Steuerungsebene werden Risiken an Dritte weitergegeben, auf der tertiären Ebene selbst getragen durch Rücklagen oder eine Berücksichtigung in den Margen.[737]

In Tabelle 13 wird unter Bezug auf alle drei Steuerungsebenen auf den in Abschnitt 5.2.2 dargestellten Prozess zurückgegriffen und beispielhaft aufgeführt, welche Möglichkeiten der Risikosteuerung im Zahlungsverkehr existieren.

Die Maßnahmen, die auf das Vermeiden und Verringern von Schadensfällen ausgerichtet sind, zielen generell auf eine verbesserte Gestaltung von Prozessen und eine Reorganisation der Unternehmen unter dem Aspekt Risikomanagement. Die meisten der aufsichtlichen Instrumente versuchen, auf diesen Ebenen anzusetzen, wie in Abschnitt 5.1 gezeigt. Meist sind die Vorgaben in Bezug auf die Verantwortlichkeit der Unternehmensleitung etwa nach § 91 AktG deutlich formuliert. Im Hinblick auf die notwendige Ausgestaltung, um dieser Verantwortung gerecht zu werden, sind die Ausführungen in den entsprechenden Gesetzen und Verordnungen eher vage – die geläufige Formulierung lautet „angemessene Verfahren auf dem Stand der Technik“ müssen angewendet werden. Dies kann einerseits mit dem liberalen Ansatz der Gesetzgebung erklärt werden, der marktwirtschaftliche Gestaltungsfreiheit nicht gefährden will, andererseits sind die auslegungsfähigen Passagen in den Vorgaben nötig, um der dynamischen Entwicklung der Märkte und Methoden gerecht zu werden. Beispiele für Spielräume bei der Interpretation finden sich unter anderem bei den Mindestanforderungen der BAFin (vormals BAKred).

Operationelle Risiken und die aufbau- und ablauforganisatorischen Anforderungen an das Risikomanagement werden am deutlichsten in den „Sound Principles for the Management and Supervision of Operational Risk“ adressiert. Grundsatz 6 lautet:[738]
“Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.”

In ihren Ausführungen zu diesem Prinzip[739] fordert die BIZ ausdrücklich starke Kontrollstrukturen für das Management Operationeller Risiken innerhalb der Kreditinstitute. Dabei wird neben schriftlich fixierten Richtlinien, Regeln und Vorschriften verlangt, ein hierarchisches Berichtswesen mit Zuweisung von Verantwortlichkeiten im Misserfolgsfall zu etablieren. Dies soll einhergehen mit einer Aufgabenverteilung, die widerstreitende Interessen in einer Funktion vermeidet.

[737] Vgl. Hofmann (2002b), S. 87 f.
[738] BIZ (2003a), S. 10.
[739] Vgl. BIZ (2003a), S. 10 ff.

Unter Bezugnahme auf die Auswertung einzelner hoher Schadensfälle in der Vergangenheit sollen die Kreditinstitute gemäß Grundsatz 6 insbesondere folgende Maßnahmen ergreifen:

- Klare Zugangs- und Zugriffsregeln zu Daten und Aufzeichnungen definieren und überwachen.
- Hinreichende Ausbildung und Training des Personals sicherstellen.
- Sonderentwicklungen in einzelnen Geschäftsbereichen als Frühwarnindikator nutzen.
- Laufende Kontrollen von Transaktionen und Konten durchführen.
- Besondere Mechanismen zur Berücksichtigung Operationeller Risiken bei Neuproduktentwicklungen, beim Erschließen neuer Geschäftsfelder und Märkte, insbesondere bei starkem Wachstum dieser Felder und bei größerer räumlicher Distanz zur Geschäftsführung, installieren.

Dem Wesen von „Principles" entsprechend sind auch diese Vorgaben nur bedingt klar und unmissverständlich umsetzbar. Verantwortungsvolles kaufmännisches Handeln sollte ohnehin diese Aspekte berücksichtigt haben. Wichtig ist in diesem Zusammenhang der Hinweis der Aufsicht, dass entsprechende gravierende und bekannt gewordene Schadensfälle nur durch Missachtung solcher vermeintlich selbstverständlicher Maßnahmen auftreten konnten.

Die Entwicklung und der Einsatz neuer Technologien und Prozesse lässt sich nicht zuletzt aus wettbewerblichen Gründen kaum aufhalten. Gleichwohl warnt die BIZ vor dem Risiko, durch die Automation von „high-frequency, low-severity"-Verlusten zu „low-frequency, high-severity"-Verlusten zu gelangen. Ein Grund mehr für ein dezidiertes Management Operationeller Risiken – und aus Sicht des Autors der Hauptgrund für die zunehmende internationale Beschäftigung mit dem Thema Operationeller Risiken. Mehr als auf diese Problematik aufmerksam zu machen, kann die BIZ an dieser Stelle (noch) nicht, da die Techniken zum Umgang mit dieser Fragestellung gerade in der Entwicklung sind.
Die Möglichkeit, die Folgen von Schadensfällen durch Operationelle Risiken auf Dritte zu überwälzen, wird von der BIZ explizit thematisiert. In den „Sound Practices" werden Versicherungslösungen als eine Alternative im Risikomanagement angesehen, unter der Maßgabe, dass die Auszahlung durch die Versicherung im Schadensfall schnell und definitiv erfolgt. Versicherungslösungen können aus Sicht der BIZ ein wirksames internes Risikomanagement nicht ersetzen und sollten auf bestimmte Schadensereignisse reduziert bleiben, u.a. Schadensersatzklagen, Naturkatastrophen und bestimmte Betrugsformen.

Volkswirtschaftlich und aus Sicht der Versicherungen betriebswirtschaftlich sind Versicherungen ohnehin nur an den Stellen sinnvoll einzusetzen, an denen die Versicherung mit versicherungsmathematischen Methoden, die auf eigenen Datenreihen basieren, adäquate Prämien in Abhängigkeit einer bestimmten Risikomanagementstruktur berechnen kann. Zu Recht macht die BIZ darauf aufmerksam, dass ansonsten Risiken lediglich in andere Sektoren transferiert werden, mit dem Problem möglicher neuer Risiken (Vertragsrisiken, Erfüllungsrisiken).[740]

Es kann erwartet werden, dass die Anforderungen, die Versicherungen an die Risikomanagementumgebung der Kreditinstitute stellen, bevor sie einer Versicherungspolice zustimmen, sich in Zukunft stark an den Vorgaben der BIZ orientieren werden. Weichen die Methoden des Kreditrisikomanagements von Basel II ab, werden die Institute nicht nur Schwierigkeiten mit der Aufsicht bekommen, die Versicherungsprämien werden voraussichtlich deutlich höher ausfallen. Die Entwicklung eigener Vorgaben aus der Versicherungsbranche, die signifikant

[740] Vgl. BIZ (2003a), S. 11.

von den Basel II Empfehlungen abweichen, wäre betriebswirtschaftlich kaum sinnvoll durchzusetzen. Dazu wäre ein alternativer Industriestandard notwendig, der in anderen Branchen bereits mit Erfolg bei Operationellen Risiken eingesetzt wird, oder zumindest kurz davor steht. Dies ist nicht der Fall, auch der ISO 17799 steckt, was die Umsetzung angeht noch in den Anfängen und die „Sound Practices“ lehnen sich ohnehin stark an diesen internationalen Standard an.

Grundsatz 7 der “Sound Practices” geht nach den allgemeinen Anforderungen von Grundsatz 6 auf die schweren Fälle von Geschäftsunterbrechungen und die dafür notwendigen Maßnahmen ein und zielt insbesondere auf die Bewältigung externer (Natur)katastrophen aber auch terroristischer Anschläge ab:[741]
„Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.”

In den Ausführungen zu Grundsatz 7 macht die BIZ deutlich, dass Banken im Bereich wahrscheinlicher Szenarios eine angemessene Reaktion auf unerwartet schwere Ereignisse vorbereiten sollten.[742] Insbesondere die mögliche Beeinträchtigung der Informationstechnologie, der Telekommunikation aber auch einzelner Gebäude sollen bei diesen Planungen im Vordergrund stehen. Ausgehend von einer Analyse kritischer Teilprozesse und Dienstleistungen, die ein Institut Dritten gegenüber vertraglich verpflichtet ist zu erbringen, sollen die Kreditinstitute alternative Verfahren vorhalten, die ohne die beeinträchtigten Infrastrukturen auskommen können. Die Sicherung und Erreichbarkeit von elektronischen Daten spielt dabei eine bedeutende Rolle. Die Katastrophenpläne sollen nach den Vorstellungen der BIZ regelmäßig den Gegebenheiten angepasst und Testläufen unterzogen werden.

Vorbeugende Maßnahmen, Notfallpläne etc. sind für seltene aber hohe Schadensfälle, seien es terroristische Aktivitäten oder Naturkatastrophen, sicherlich notwendig. Gleichwohl sollte der Effekt der Solidarität bei Schadensfällen, die weltweit Aufsehen erregen, nicht unterschätzt werden. Der Großzahlungsverkehr beispielsweise hätte theoretisch am 11. September 2001 durch die weltweiten Abhängigkeiten beträchtlichen Schaden nehmen können. Durch extrem kurzfristige und teils informelle Absprachen und Garantien – sowohl auf Seiten der Geschäftsbanken als auch bei den Zentralbanken – ist auf der Seite der systemischen Risiken wirkungsvoll ein Großschaden vermieden worden, obwohl in diesem Ausmaß keinerlei Notfallplan weder theoretisch angedacht noch praktisch eingeübt worden war.[743]

[741] BIZ (2003a), S. 12. Die Ausführungen sind sichtlich von den Erfahrungen des 11. September in New York beeinflusst.
[742] Vgl. BIZ (2003a), S. 12.
[743] Vgl. in diesem Zusammenhang das Beispiel von Barvell (2002), S. 1, der auf die Tatsache aufmerksam macht, dass die Federal Reserve Bank of New York nach dem 11.09.2001 bis zu USD 81 Mrd. an Übernachtkrediten vergab, um die Teilnehmer an Großzahlungssystemen liquide zu halten. Normalerweise vergibt die Federal Reserve Bank solche Kredite nicht.

Risiko...	Beispiele
...vermeiden durch:	Einführung neuer Techniken, bspw. „SecureCode“ von MasterCard oder „Verified by Visa“ – bei gleichzeitiger Absicherung gegen neue mögliche Probleme durch diese Verfahren. Vermehrte Zusammenarbeit der Kreditinstitute im Zahlungsverkehr, zur Früherkennung z. B. von Betrugsmustern wie institutsübergreifendem Lastschriftbetrug. Werden potenzielle Angriffsmöglichkeiten durch Betrüger ebenso wie mögliche Systemschwachstellen bei elektronischen Prozessen instituts-übergreifend kommuniziert, können die Institute eigenständig mögliche Gefahren gewichten und Gegenmaßnahmen ergreifen, bevor es zu Schadensfällen kommt. Beispiel: Virenwarnungen und Angebot von entsprechenden Patches oft bevor die Rechner infiziert sind. Im Großzahlungsverkehr durch Abbau alternativer Kanäle, die bis dato immer wieder Ausnahmen von standardisierten und sicheren Prozessen ermöglichen.
...vermindern durch:	Nach Analyse aufgetretener Schäden kann die Ursache für mögliche zukünftige Schäden beseitigt werden. Neben kontinuierlicher Analyse von Schadensfällen, können Präventionsmaßnahmen durch gezielte Prozessanalyse realisiert werden, z. B. Aufdecken der Möglichkeit gefälschter Bestätigungsmails der erfolgten Bezahlung an den Händler. Personal kann gezielt geschult werden, beispielsweise Betrugsfälle, interne und externe, zu erkennen, zu bewerten und in Datenbanken zu erfassen. Ausbau der Qualitätssicherung bei Neuproduktentwicklung und Alltagsprozessen.
...überwälzen auf:	Spezielle Versicherungen gegen Operationelle Risiken, bspw. Zurich International E-Risk-Edge. Allerdings können die Vertrags-Klauseln unter Umständen auch sehr rigide Formulierungen in Bezug auf das notwendige Risikomanagement enthalten. Zudem besteht nach Schadensfällen in der Regel eine Kündigungsmöglichkeit. Eine andere Möglichkeit besteht in der Inanspruchnahme von Dienstleistern, z. B. kann das Inkasso bei einem Zahl-Verfahren von Dritten geleistet werden, die Forderungen der Händler zu einem bestimmten Preis aufkaufen. Das Kreditinstitut vermittelt dann nur diese Dienstleistung. Nachteil: weniger Marge.
...selbst tragen:	Ein Restrisiko für das Eintreten unerwarteter Verluste bleibt immer bestehen. Es kann nur versucht werden, dieses auch im Zahlungsverkehr möglichst gering zu halten. Die kalkulierbaren Risiken wie beispielsweise bisher stattfindender Kreditkartenbetrug können über die Marge getragen werden. Allerdings nur, wenn sich die Betrugsmethoden und Haftungsbedingungen nicht zu Ungunsten der Kreditinstitute weiter entwickeln. Die Unterlegung unerwarteter Verluste durch Operationelle Risiken mit Eigenkapital stellt den Kern der Überlegungen in Basel II dar.

Tabelle 13: Maßnahmen des Risikomanagements im Zahlungsverkehr auf Seiten der Systemanbieter

Diese Aussage soll die Notwendigkeit von Notfallplänen nicht relativieren. Es soll lediglich darauf hingewiesen werden, dass vermutete systemische Risiken mit negativen Auswirkungen beispielsweise auf das Vertrauen in die Zahlungssystemlandschaft, eher durch betrügerische Aktionen und informationstechnologische Fehler und Pannen wirksam werden als durch katastrophale Großereignisse. Diese wirken durch die ausgelöste Welle der Solidarität zunächst in positivem Sinne gegen systemische Unsicherheiten.

Eine weitere positive Verstärkung erfahren die Finanzsysteme durch die Konsequenzen, die aus bereits durchlebten Krisen und Katastrophen gezogen wurden. Beispielsweise haben die notwendigen tiefgreifenden IT-Systemumstellungen im Rahmen der Jahr 2000-Problematik vermutlich einen entscheidenden Anteil an einem weniger dramatischen Verlauf der Ereignisse des September 2001. Die weite räumliche Trennung redundanter Einheiten wiederum ist erst eine Folge der Erfahrungen aus diesem September, hat aber dennoch zur Folge, dass beispielsweise lokale Naturkatastrophen bestimmte Fehlertypen nicht mehr hervorrufen können, die durch enge räumliche Konstellationen von Systemen und Reservesystemen denkbar waren.

5.3.2.4 Management Operationeller Risiken und Kontrolle

Die ersten drei Grundsätze der „Sound Principles“ legen den generellen Rahmen und Verantwortlichkeiten im Bereich des Managements Operationeller Risiken fest, Grundsatz 4 betont die Notwendigkeit der Quantifizierung von Operationellen Risiken. Erst Grundsatz 5 bildet die Leitlinie für die Kontrolle und das Management dieser Risiken:[744]
„Banks should implement a process to regulary monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.”

Diese Ausführungen sind noch ähnlich vage wie die entsprechenden Formulierungen des KonTraG. Die Ausführungen zum Grundsatz 5 konkretisieren die Absicht der BIZ.[745] Zunächst soll ein kontinuierlicher Überwachungsprozess in den Finanzinstituten installiert werden, der eine Warnung an die entsprechenden verantwortlichen Stellen ermöglicht, falls es zu Unregelmäßigkeiten im Tagesgeschäft kommt. Ergänzt werden sollen solche Überwachungsprozesse um mögliche Frühwarnindikatoren, die der Geschäftsführung rechtzeitig mögliche Gefahren im Bereich der Operationellen Risiken signalisieren. Beispielhaft für diese Indikatoren nennt die BIZ die Einführung neuer Produkte, die unerwartet starke Expansion einzelner Geschäftsfelder, unerwartete Fluktuationsraten beim Personal oder IT-Systemkennziffern wie Ausfallzeiten. Gibt es gesicherte Erkenntnisse über Korrelationen von Schadensfällen in der Vergangenheit mit den Indikatoren, kann die Geschäftsführung bei Überschreiten bestimmter – vorher festgelegter Kennzahlen – unmittelbar Maßnahmen ergreifen.

Funktional sollten die Überwachungsaufgaben je nach Gefährdungslage ins Tagesgeschäft mit Berichtspflichten (bis hin zu Berichten für die Aufsicht) integriert sein und ebenso regelmäßigen internen Audits durch die Revisionsabteilung oder anderen Verantwortlichen des Risikomanagements unterliegen.

Die weiteren Vorgaben an ein Management-, Überwachungs- und Kontrollsystem für Operationelle Risiken ähneln sehr stark analogen Vorgaben für andere Risikomanagementbe-

[744] BIZ (2003a), S. 9.
[745] Vgl. BIZ (2003a), S. 9 ff.

reiche, beispielsweise den Kreditrisiken. Unter anderem sollen bis hinauf zum Vorstand alle Verantwortlichen regelmäßig Statusberichte erhalten, die aufgetretene Problemfelder erläutern oder Anregungen geben, erwartete Schwierigkeiten zu bewältigen.

Die BIZ legt in ihren Anforderungen Wert auf eine Überprüfung der Überwachungsfunktionalitäten im Management Operationeller Risiken. Insbesondere haben die Finanzinstitute sicherzustellen, dass unter anderem aktuelle Entwicklungen und neue Produkte kurzfristig in die Risikobetrachtungen mit einbezogen werden. Die aufsichtlichen Anforderungen an das Monitoring des Gesamtprozesses können als Auftrag zur Implementierung von Qualitätssicherungsmaßnahmen im Management Operationeller Risiken verstanden werden. Es können institutsinterne und externe Kontrollansätze unterschieden werden.

5.3.2.4.1 Institutsinterne Ansätze der Kontrolle

Die aufsichtliche Problematik der Überprüfung der eigenen Normen und Vorgaben haben institutsintern die Revisionsabteilung und Auditoren. Angesichts der skizzierten Veränderungen ist es folgerichtig, dass die Bank für Internationalen Zahlungsausgleich die Beziehungen zwischen allen Prüforganen, den internen Auditoren in Finanzinstituten, den externen Prüfern, beispielsweise Wirtschaftsprüfungsgesellschaften, und den Aufsichtsbehörden zum Gegenstand einer Untersuchung gemacht hat.[746] Bei allen nationalen Unterschieden ist es der BIZ gelungen, für die Gestaltung interner Auditprozesse zwanzig Grundsätze im Sinne von „best practices“ zu formulieren, deren Umsetzung in den Finanzinstituten wiederum zur aufsichtlichen Aufgabe wird.

Dabei rückt die Frage der quantitativen Überprüfbarkeit interner Auditoren und Prozesse in den Hintergrund. Die BIZ stellt im Rahmen der eigenen Untersuchungen selbst fest:[747]
„Finally, co-operation between the supervisor, the internal auditor and the external auditor optimises supervision.“

Grundsätzlich geht der Trend bei Audits, externen wie internen, hin zu risikoorientierten Audits, beispielsweise der Überprüfung der institutsintern verwendeten Modelle;[748] eine Entwicklung, die durch die Betonung Operationeller Risiken in Basel II verstärkt werden wird.

5.3.2.4.2 Externe Überprüfung des Managements Operationeller Risiken

Die Pflichten der Aufsicht und auch mögliche Formen der Aufsicht wie die sogenannte „Off Site“ oder „On Site“ Prüfung sind seit längerem Gegenstand aufsichtlicher Gremien in allen Bereichen der Arbeit der Aufsichtsorgane. Die BIZ hat mit der Veröffentlichung der „Core Principles for Effective Banking Supervision“ im September 1997 sehr detailliert und zeitlos die Anforderungen an diese Arbeit formuliert.[749]

Gleichwohl wird die aufsichtliche Überprüfung der gewählten Managementansätze (nicht nur für Operationelle Risiken) und deren Implementierung im Rahmen von Basel II weiterentwickelt. Mit dem Supervisory Review Process, der die Basis der zweiten Säule bildet, wird ein

[746] Vgl. BIZ (2001h). Seit Ende der neunziger Jahre wird dieses Thema von der Aufsicht verstärkt adressiert: Vgl. u.a. BIZ (1999b), BIZ (1998d), BIZ (2002), BIZ (2002f).
[747] BIZ (2001h), S. 1.
[748] Vgl. BIZ (2002f), S. 9.
[749] Vgl. BIZ (1997).

neues fortlaufendes Verhältnis zwischen Aufsicht und Beaufsichtigten etabliert.[750] Laufende vor Ort Prüfungen durch Mitarbeiter der Aufsicht lassen die ex-post Kontrolle an Bedeutung verlieren; eine Folge zunehmend komplexer Strukturen, die nicht hinreichend in einem „Off Site“ verfassten Jahresendbericht abgedeckt werden können.

In den „Sound Principles“ finden sich mit den Grundsätzen 8 und 9 zwei Grundpfeiler für das neu formulierte Verständnis der Aufsicht bei der Überwachung der Finanzinstitute. Grundsatz 8 fordert von den Bankenaufsehern:[751]
„Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.“

Entgegen der im Umfeld von Basel II geäußerten Beschränkung der Basel II Vorgaben auf international operierende Großbanken wird im achten Grundsatz deutlich gemacht, dass ein aufwändiges Management Operationeller Risiken in Zukunft von allen Finanzinstituten gefordert wird. Diese Forderung stimmt überein mit den Ansprüchen, die von der Aufsicht im Rahmen von Basel II an die Berechnung der Eigenkapitalunterlegung gestellt werden (siehe Abschnitt 5.3.2.2). Dort wird von den Finanzinstituten die Umsetzung der „Sound Practices“ bereits auf der untersten Stufe des Basisindikatoransatzes erwartet. Einzige Einschränkung: Das Risikomanagement sollte der Größe, Bedeutung und Risikoexponiertheit des Finanzinstituts angemessen sein. Die Bedeutung der Integration des Managements Operationeller Risiken in die Gesamtprozesse, die ohne einen fortgeschrittenen Ansatz kaum vorstellbar ist, wird an anderer Stelle jedoch nochmals betont.[752]

Eine proaktive Rolle jedoch sieht die BIZ für die Aufsichtsorgane vor, falls Operationelle Risiken ein Institut substanziell bedrohen. Die Aufsicht soll dann die Finanzinstitute dabei unterstützen, bessere Verfahren für das Risikomanagement zu entwickeln und anzuwenden. Wie diese Unterstützung aussieht, bleibt bei den Ausführungen der BIZ offen. Es wird lediglich generell angedacht, die Aufsichtsorgane als Feedback-Organisation zu verstehen, die durch die Kontakte zu allen Instituten einzelnen Unternehmen eine Art Benchmark nennen kann.

Die Möglichkeit jedoch, zu beurteilen, ob die angewendeten Verfahren zum Management Operationeller Risiken angemessen sind, wird der Aufsicht mit viel Gestaltungsspielraum in der Auslegung, in die Hand gegeben. Grundsatz 9 der „Sound Practices“ fordert:[753]
„Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank’s policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.”

Die Aufsichtspflichten, die von der BIZ den nationalen Aufsichtsbehörden auferlegt werden, sind analog zu denen, die im Bereich des Managements von Marktpreis- und Kreditrisiken zu finden sind. Die Kriterien, nach denen die Aufsicht die Finanzinstitute überprüfen sollen, sind bereits ziemlich konkret, auch wenn die Überprüfung qualitativer Vorgaben einen weiteren Interpretationsspielraum lässt als dies bei quantitativen Kennzahlen der Fall ist.[754]Im Kern obliegt es der Aufsicht, die in den ersten sieben Grundsätzen geforderten Rahmenbedingun-

[750] Vgl. BIZ (2001a).
[751] BIZ (2003a), S. 13.
[752] BIZ (2003a), S. 14.
[753] BIZ (2003a), S. 13.
[754] BIZ (2003a), S. 13 f.

gen und Ausprägungen des institutseigenen Managements Operationeller Risiken auf seine Effektivität und Qualität hin zu überprüfen, angefangen bei der Durchgängigkeit des Risikomanagementprozesses vom Produkt bis zum Vorstand bis hin zu angemessenen Notfallplänen. Ein weiterer Punkt ist die Übereinstimmung der tatsächlichen Unterlegung Operationeller Risiken mit Eigenkapital mit den errechneten Risiken und dem dazugehörigen Risikoprofil.

Wer die aufsichtliche Überprüfung der Finanzinstitute vornimmt, bleibt den nationalen Aufsichtsorganen überlassen. Es können sowohl aufsichtseigenes Personal als auch externe Prüfer eingesetzt oder beauftragt werden.

Der Supervisory Review Process, in der zweiten Säule von Basel II angelegt, ist bereits in den Ausführungen zu Grundsatz 9 spürbar. Anstelle quartalsbezogener oder jährlicher Prüfberichte nach Einreichung der Unterlagen wird eine direkte Einbindung der Aufsicht in das Berichtswesen der Finanzinstitute angedacht: „for example, internal bank management reports on operational risk could be made routinely available to supervisors“[755].

Dieser Gedankengang der Aufsicht verdeutlicht, welcher Paradigmenwechsel bei der Beziehung von Aufsicht zu Finanzinstituten durch Basel II angestoßen werden könnte. Für die Institute ist die Vorstellung, die Aufsicht an das Berichtswesen des Vorstands angedockt zu sehen, sicherlich keine ganz alltägliche. Wird von der Aufsicht diese Erwartung formuliert, ist auf der anderen Seite allerdings auch deutlich, dass eine Alternativlösung – zwei verschiedene Berichte für Aufsicht und Vorstand – seltsam anmuten würde. Kann ein Institut nicht glaubhaft machen, dass ureigene Geschäftsinteressen einer „Veröffentlichung“ der Lageberichte entgegenstehen, würde der Eindruck entstehen, bestimmte Operationelle Risiken würden an der Aufsicht vorbei „geschleust“.

Die Kontrolle durch die Aufsicht hat mit Basel II durch die geplante dritte Säule, die Offenlegung von institutsrelevanten Informationen, eine weitere Dimension erhalten. Grundsatz 10 der „Sound Practices“ fordert:[756]
„Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.”

Noch gibt auch die Aufsicht unumwunden zu, wäre es zu früh, den Instituten vorzugeben, welche relevanten Informationen sie der Öffentlichkeit über Operationelle Risiken und deren Management zu geben haben.[757] Aber für den Fall, dass die Aufsicht mit den Anstrengungen der Institute nicht zufrieden ist, lässt sich diese Säule durchaus für die Institute nachteilig ausbauen.

5.3.3 Kritische Würdigung des Operational Risk Management-Ansatzes in Basel II und Entwicklung eines weiterführenden Ansatzes im Bereich Zahlungsverkehr

Der Umgang mit Operationellen Risiken als institutsweiter Prozess ist bislang noch in keiner Regulierung, weder national noch international, so umfassend wie in den Entwürfen zu Basel II thematisiert worden.

Die bestehenden Probleme bei der Datenerfassung und der Bezug der Arbeiten zu Operationellen Risiken in Basel II haben das Hauptaugenmerk praktisch aller Publikationen auf die

[755] BIZ (2003a), S. 13, Ziffer 48.
[756] BIZ (2003a), S. 14.
[757] BIZ (2003a), S. 14.

Quantifizierungsansätze dieser Risiken gelegt. Aus Sicht des Autors ist dies in einer ersten Stufe legitim. Gemäß dem Diktum „Miss es oder vergiss es!“[758] ist die Bewertung von Risiken in Geldeinheiten für jeden adäquaten Steuerungsprozess eine unabdingbare Voraussetzung.

Allerdings sollten nach Meinung des Autors die Ansätze zur Identifizierung und Analyse Operationeller Risiken im laufenden Geschäft nunmehr in den Vordergrund rücken. In Basel II wird gegen Ende der dritten Konsultationsphase davon ausgegangen, dass diese Arbeit von den Kreditinstituten zu leisten ist, und das Ergebnis von der Aufsicht „lediglich“ überprüft wird. Im Rahmen des Supervisory Review Process wird diese Überprüfung eine laufende Vor-Ort-Überwachung durch die Aufsicht beinhalten.

Im folgenden wird ein Ansatz mit den notwendigen Voraussetzungen vorgestellt, der einem kooperativen Ansatz folgend die Chancen aufzeigt, die bei der Bewältigung Operationeller Risiken in einem einheitlichen Vorgehen genutzt werden können.

5.3.3.1 Argumente für ein kooperatives Vorgehen beim Management Operationeller Risiken

Es lassen sich verschiedene Argumente unterscheiden, die einen kooperativen Ansatz beim Management Operationeller Risiken unterstützen (siehe Tabelle 14). Kooperativer Ansatz meint in diesem Zusammenhang die Zusammenarbeit der Finanzinstitute bei der Datensammlung und –analyse und parallel die Integration der Aufsichtsorgane in diesen Prozess.

Aus strategischer Sicht ist die Erkenntnis von Bedeutung, dass die Bewältigung Operationeller Risiken nicht zum Kerngeschäft der Finanzinstitute gehört. Das Management Operationeller Risiken ist im Gegensatz zum Management von Markt- und Kreditrisiken eher ein notwendiges Übel. Für den Zahlungsverkehr ist das Management Operationeller Risiken gleichwohl nicht nur aufgrund der entstehenden Kosten von Bedeutung. Die systemischen Risiken einerseits und die empfindliche Reaktion der Öffentlichkeit auf (medienwirksame) Probleme im Bereich elektronisches Bezahlen betonen zusätzlich die Notwendigkeit effektiver Managementansätze – auch wenn Reputationsrisiken nicht zu den Operationellen Risiken gezählt werden aber im Zahlungsverkehr eng mit den systemischen Risiken korreliert sein dürften. Eine besonders effiziente Bewältigung Operationeller Risiken scheint bei der derzeitigen Ausgestaltung des Anreizsystems für die Finanzinstitute zur Eigenmittelunterlegung nach den geschilderten Ansätzen nicht so lohnend, dass die Finanzinstitute auf eine branchenbezogene Zusammenarbeit verzichten würden, um einen Wettbewerbsvorteil zu erzielen. Der Erfolg einer ohnehin vermutlich unlauteren Werbung der Art „Bei uns ist Ihr Geld nicht so stark gefährdet wie bei der Konkurrenz!“ darf bezweifelt werden.

Der Intrabranchen-Wettbewerb dürfte für ein erfolgreiches Management Operationeller Risiken kontraproduktiv sein. Anders sieht es bei einem zunehmenden Interbranchen-Wettbewerb aus. Ein zusätzliches Motiv zur effektiven Bewältigung der Herausforderungen durch Operationelle Risiken stellen die in Kapitel 4.2.6.5 aufgezeigten strategischen Ausrichtungen potenzieller Akteure auf dem Zahlungssystemmarkt dar. Gelingt es den Finanzinstituten als strategischer Gruppe, ein besonders effektives Risikomanagement aufzubauen, gerade in den Schadenskategorien Betrug und Datenverarbeitung, könnten sie sich unter Umständen besser – unter anderem wegen der geringeren Schadenssumme – gegen die neu hinzukommende Konkurrenz positionieren, die zunehmend auf die gleichen Risiken stoßen dürfte wie die Finanzinstitute. Die Flexibilität der neu auf den Markt drängenden

[758] Stögbauer (2002).

Konkurrenz kann im Bereich Operationeller Risiken ein funktionierendes Netzwerk zur Schadensbegrenzung entgegengesetzt werden.

Quantifizierung ist nur der erste Schritt, dieser Datenpool muss analysiert werden.
Das erfolgreiche Management Operationeller Risiken ist kein notwendiges Differenzierungsmerkmal zur Konkurrenz.
Erfolgreiche Bewältigung Operationeller Risiken kann jedoch branchenfremde Wettbewerber unter Umständen fernhalten.
Selbstregulierung der Finanzwirtschaft und Kooperation mit der Aufsicht nehmen auf der Agenda von Basel II prominente Plätze ein. Der Supervisory Review Process wird in der zweiten Säule von Basel II verankert.
Die Quantifizierung der Operationellen Risiken generiert Daten, deren Analyse institutsübergreifend einen beträchtlichen Mehrwert bieten können.
Die Aufsicht könnte ihr Image von der Pflichten auferlegenden Institution hin zu einer auch Mehrwert vermittelnden Institution wandeln.

Tabelle 14: Argumente für einen kooperativen Ansatz zur Bewältigung Operationeller Risiken

Basel II und weitere aktuelle Entwicklungen auf nationaler und europäischer Ebene der Regulierung erhöhen den Druck auf die Finanzinstitute. Die Aufsichtsbehörden in Europa sind sich der möglichen Risiken im Zahlungsverkehr, neuerdings auch im Massenzahlungsverkehr, zunehmend bewusst und behalten sich aufsichtliche Schritte der Regulierung vor, für den Fall, dass die bankinternen Maßnahmen nicht ausreichen.[759] Wie in Abschnitt 6.3.1 weiter ausgeführt sind in einzelnen Ländern, z. B. in Frankreich, die Aufsichtsorgane im Bereich Retail-Bezahlverfahren bereits deutlich aktiver als die Diskussion in Deutschland oder auf europäischer Ebene vermuten lässt.

Die Anforderungen an die Aufsicht selbst werden in den letzten Jahren immer höher. Die BIZ formuliert dazu:[760] „Darüber hinaus hinkt eine Eigenkapitalregelung, selbst eine so zukunftsorientierte Regelung wie die Neue Basler Eigenkapitalvereinbarung, zwangsläufig hinter den sich verändernden Risikoprofilen von komplexen Bankkonzernen her, vor allem wenn diese von neuen Geschäftsmöglichkeiten Gebrauch machen.“ Somit ist es erklärlich, dass mit Basel II und dem Supervisory Review Process das bisher unterbetonte Element kontinuierlicher Überwachung mit kooperativen Zügen bei der Weiterentwicklung der aufsichtlichen Methoden ein stärkeres Gewicht bekommt.

Diese Rahmenbedingungen können so interpretiert werden, dass die Finanzinstitute zumindest im Bereich des Zahlungsverkehrs ein gemeinsames Interesse an der Bewältigung Operationeller Risiken haben sollten. In Deutschland ist durch die geschilderte Sonderstellung des Bankensektors im Wettbewerbsrecht eine gemeinsame Zusammenarbeit mit der Aufsicht beispielsweise im ZKA prinzipiell nicht nur möglich, sondern sogar erwünscht. Auf

[759] Vgl. Fabritius (2003a), S. 4 f.
[760] BIZ (2003c), S. 12.

europäischer Ebene deuten institutionelle Entwicklungen, z. B. die gelungene Etablierung des European Payments Council, auf ähnliche Strukturen und Möglichkeiten der Kooperation hin. Die Erwartungshaltung an eine zielgerichtete Arbeit des EPC gerade im Hinblick auf Selbst-Regulierung aber auch auf potenzielle Zusammenarbeit mit der Aufsicht ist auf aufsichtlicher Seite bereits aufgrund der weiteren Entwicklung des gemeinsamen europäischen Währungsraums dementsprechend hoch.[761] Noch sind auf der politischen Agenda die Ziele der Single European Payment Area fundamentaler Art. Zunächst soll in der Eurozone eine transnationale Infrastruktur etabliert werden. Es liegt nahe zu vermuten, dass in einer zweiten Stufe Sicherheitsfragestellungen und das länderübergreifende Management Operationeller Risiken insbesondere im Zahlungsverkehr – beispielsweise beim Missbrauch der geplanten europäischen Lastschrift – eine wichtige Rolle einnehmen werden.

Der Vorteil einer im weiteren vorgeschlagenen Zusammenarbeit der Finanzinstitute bei der Identifikation, Analyse und Bewältigung bestimmter Operationeller Risiken ist neben einer möglichen institutsinternen Reduktion von Schäden durch diese Risikoart eine mögliche Integration der Aufsicht in diese Prozesse. Diese Integration könnte in beiderseitigem Interesse sein. Bei einer branchenweiten Analyse Operationeller Risiken und daraus resultierenden Ergebnissen, beispielsweise Frühwarnungen, können die Finanzinstitute schneller auf Gefahren und Angriffe reagieren. Die Aufsicht als integraler Bestandteil eines solchen Analyse- und Auswertungssystems erhält ein branchenweites Gespür für jeweils aktuelle und relevante Problemlagen und kann die erfolgreichen Bemühungen der Institute auf Operationelle Risiken zu reagieren direkt mitverfolgen. Für die Institute würde aus der Kooperation mit der Aufsicht ein Mehrwert entstehen, den eine wettbewerbliche Lösung – Datensammlungs- und Analysekonsortien mit regionalen oder branchenspezifischen Schwerpunkten – vermutlich in dieser umfassenden Form nicht bieten könnte. Für die Aufsicht könnte im Erfolgsfall das Image einer Institution, die ständig den Instituten neue Pflichten auferlegt und Kosten verursacht, hin zu einer mehrwertvermittelnden Organisation verändert werden.

Wird bei den Arbeiten im Rahmen von Basel II ein Schwerpunkt auf die Quantifizierung der Schäden durch Operationelle Risiken gelegt, steht bei diesem Vorschlag die gemeinsame Datenanalyse durch die Kreditinstitute und die Aufsicht im Vordergrund. Durch umfangreiche bankenübergreifende Datenanalysen können potenzielle Schäden und Schadenszusammenhänge unter Umständen früher erkannt werden. Insbesondere sind Schadensmuster, z. B. bestimmte Angriffsstrukturen auf Kreditkartensysteme, an einer Stelle erkennbar und analysierbar und können im Netz der angeschlossenen Organisationen weitergegeben werden, um ähnliche Schadensfälle zu erkennen.

In Deutschland gibt es im Bereich Zahlungsverkehr eine historisch gewachsene Komplementarität zwischen der Zentralbank und dem Geschäftsbankensektor.[762] Diese zumindest in einigen Ländern des Eurosystems bei Fragen der Effizienz und Zuverlässigkeit der Zahlungssysteme funktionierende Kooperation könnte im Bereich der Operationellen Risiken bezüglich der Datensammlung aber vor allem der Analyse und Hilfestellung nach Meinung des Autors weiter ausgebaut werden.

Die Natur der Operationellen Risiken macht rein quantitative Ansätze des Risikomanagements diffizil; damit wird allerdings auch die schematische Überprüfbarkeit aufsichtlicher Regelungen schwierig. Ein alternativer Ansatz, der auf weitergehender Kooperation zwischen Zentralbank(en) und Geschäftsbanken für das Management Operationeller Risiken beruht,

[761] Vgl. Fabritius (2003a), S. 4.
[762] Vgl. Fabritius (2003a), S. 6.

wird für den Bereich elektronischer Zahlungsverkehr im folgenden exemplarisch dargestellt. Beispielanalysen können aufgrund der nicht öffentlich verfügbaren Daten nur angedeutet, aber nicht empirisch bestätigend durchgeführt werden.

5.3.3.2 Datenlage und die mögliche Rolle der Aufsicht

Setzen sich zur Quantifizierung der Risiken die VaR-Ansätze durch, kann bei allen Unterschieden in den Risikoarten aus der historischen Entwicklung der Modelle für Markt- und Kreditrisiken gelernt werden. Ein wesentlicher Bestimmungsfaktor für die Qualität von Berechnungsmodellen ist neben der Standardisierung von Daten die historische Verfügbarkeit verschiedener Indikatoren, die (vermutlich) einen Einfluss auf die zu schätzende Variable haben. Erst dann kann erfolgreich getestet und der vermutete Einfluss einzelner oder mehrerer Indikatoren empirisch belegt werden.[763] Die Erfahrung bei der Modellierung von Kreditrisiken zeigt, dass sich erst nach einigen Jahren die Schwächen fehlender Daten insbesondere Indikatoren zeigen. Dies führt im Hinblick auf die Zuverlässigkeit dieser Ansätze zu erheblichen Problemen. Bei einer Aufzählung einiger beispielhafter Schwierigkeiten bei der Modellierung von Kreditrisiken im VaR-Verfahren sind diese, sofern der jeweilige Begriff der Terminologie Operationeller Risiken angepasst wird, ebenso für Operationelle Risiken von Bedeutung:

- "Die Datenbasis für Kreditausfälle und Wiedergewinnungsraten sind viel unvollständiger als im Marktrisikobereich. Interne Daten der Kreditinstitute sind häufig nicht in einer auswertbaren Form zusammengestellt [...].
- Es gibt nur wenig Informationen über den Einfluss von Makrofaktoren wie die Konjunktur, die geographische Lage, den Industriezweig oder die Fristigkeit des Kredits auf den Kreditausfall und die Wiedergewinnungsraten.
- Die Spärlichkeit des Datenmaterials kennzeichnet auch die Korrelation zwischen Kreditrisiken, die sich daher auf Ersatzvariablen wie die Korrelation der Aktienrenditen, die Korrelation von Anleihespreads oder die Korrelation zwischen Produktionsziffern von Industriezweigen stützen muss. Ob diese Ersatzvariablen den tatsächlichen Risikozusammenhang von Kreditpositionen annähernd beschreiben können, ist unklar."[764]

Nach Einschätzung des Autors können einige der oben aufgeführten Probleme, insbesondere die schwierige Datenlage, zum gegenwärtigen Zeitpunkt für den Bereich Operationeller Risiken erfolgreich reduziert werden.

Für die Operationellen Risiken geht die BIZ mit den QIS und der Loss Data Collection Exercise for Operational Risk (LDCE) in die richtige Richtung. Zum ersten Mal werden branchenweit standardisierte Vorgaben zur Erhebung Operationeller Risiken gemacht. Diese Daten können aber, sollen sie nicht „nur" der Quantifizierung dienen, nur dann zur Analyse von Schadensfällen und als Input für Frühwarnsysteme dienen, wenn zumindest versucht wird, weitere aussagekräftige Parameter mit zu erheben.

Die QIS und die darunter liegenden Teiluntersuchungen wie die LDCE sind auch nach Ansicht der BIZ nicht endgültig fixiert. Die Daten der einzelnen Vergleichserhebungen sind bislang nur sehr bedingt vergleichbar, da nicht nur die Teilnehmerzahlen stark zugenommen haben, sondern zusätzlich das verstärkte Bemühen um die Erfassung Operationeller Risiken

[763] Vgl. zur Entwicklung der Modelle bei Default Rates von Krediten Rudolph (2000), S. 31 f.
[764] Rudolph (2000), S. 45 f.

innerhalb der Finanzinstitute eine zeitliche Dateninkonsistenz bewirkte.[765] Insofern befindet sich die BIZ bei der systematischen Erhebung Operationeller Risiken gleichsam in der Stunde Null, verfügt jedoch als einzige supranationale Institution über sehr viel Erfahrungswissen durch die bis Sommer 2003 durchgeführten vier QIS.

Erste Diskussionen um die Datenqualität und eine mögliche Erweiterung der gesammelten Parameter bei Operationellen Risiken hat die BIZ bereits Ende 2001 im ersten Entwurf zu den „Sound Practices" angestoßen.[766] Die BIZ macht auf die Schwierigkeiten statistischer Überprüfungsverfahren wegen mangelnder Datenanzahl aufmerksam. Insbesondere Back-testing-Verfahren machen nur bei vollständiger Datenlage und genügend Datenpunkten Sinn, bei „low frequency – high impact"-Schäden ist dies eine schwierig zu erfüllende Bedingung.

Eine große Schwierigkeit stellt bei kostenintensiven Maßnahmen, die ein Mehr an Sicherheit ermöglichen sollen, die fehlende Vergleichbarkeit innerhalb einer Branche aber auch branchenübergreifend dar. Es fehlen weitgehend, beispielsweise im ablauforganisatorischen Bereich der IT-Sicherheit, Benchmarking-Größen, an denen sich Fachverantwortliche und Management bei der Allokation von Ressourcen orientieren können. Gerade Benchmarking-Kennzahlen und „best practices" sind in der Risikomanagement-Landschaft gern gesehen. Allerdings wird vielfach zunächst der Vorschlag gemacht, die Finanzinstitute sollten ihre eigenen Klassifizierungen und Methoden verwenden.[767] Wird nicht parallel – eine betriebswirtschaftlich bei derart komplexen Vorgängen unsinnige Lösung – mit einem standardisierten Vorgehensmodell gearbeitet, werden Benchmarking und „best practices" zumindest fragwürdig, wenn nicht substanzlos. Bei den QIS hat es sich als wesentliches Hindernis bei der Analyse der Daten herausgestellt, dass bereits einfache Festlegungen wie die meldepflichtige Mindestschadenssumme bei Differenzen von Institut zu Institut gravierende Auswirkungen auf die Datenqualität haben.

Die Frage, wer die Indikatoren festlegt, und wer die Daten erhebt sowie auswertet, ist eine zentrale Bestimmungsgröße möglicher späterer Erfolge zur Bewältigung Operationeller Risiken. Nur wenn es gelingt, eine standardisierte Berichtsform einzuführen, und entsprechend konsensfähige Indikatoren in einer festgelegten Detailtiefe abzufragen, kann dieser Datenpool a) sinnvoll ausgewertet werden und b) den Instituten die Notwendigkeit einer solchen Datenerhebung verständlich gemacht werden.

Nur ein standardisiertes Vorgehen durch einen neutralen Dritten, den die Aufsicht darstellen könnte, kann auf mittlere Sicht der Kritik an den bisherigen Ansätzen zur Quantifizierung Operationeller Risiken, wirksam begegnen. Beeck und Kaiser kritisieren beispielsweise bei allen Methoden, die sich vor der Einführung der QIS mit der Thematik beschäftigten, die fehlende einheitliche Klassifizierung, die Subjektivität von Experteneinschätzungen, die prohibitiven Kosten bei einer Einzelprozessanalyse und die fehlende Anzahl an Datenpunkten für die erfolgreiche Anwendung statistisch-versicherungsmathematischer Methoden.[768]

Ein zentralisierter Erhebungsansatz löst nicht die Problematik einer einheitlichen Erhebungssystematik. Solange der Begriff der Operationellen Risiken noch relativ jung ist, wird die Interpretation von Ereignissen, die Quantifizierung und auch die Ursachenanalyse hinreichend subjektive Elemente enthalten, um für Verzerrungen im Datenmaterial zu sorgen. Unter anderem spielt bei branchenweiter Datensammlung die jeweilige Risikokultur der Finanzinsti-

[765] Vgl. BIZ (2003g), S. 4 und BIZ (2002a).
[766] Vgl. BIZ (2001l), S. 22.
[767] Vgl. Peter (2000), S. 665 f.
[768] Vgl. Beeck (2000), S. 640 ff.

tute eine gewichtige Rolle. Verschiedene Fragen sind von Bedeutung für die Interpretation der Daten. Beispielsweise muss geklärt werden, ob die Institute bereits vorher ein Berichtswesen etabliert hatten? Oder werden Mitarbeiter für das Aufdecken von Problemen und Schadensfällen eher belohnt oder sanktioniert?

Vermutlich wird sich eine gewisse Homogenität der Datensätze erst über die Jahre einstellen, und umso eher, je intensiver die Aufsichtsbehörden einheitliche Leitlinien herausgeben. Nicht jedes Finanzinstitut ist im Bereich Operationeller Risiken so weit wie die Bayrische Landesbank, die bereits seit Ende 1999 das Thema adressiert und in Projekten umsetzt. Stocker et al. machen in ihrem Bericht auf die Schwierigkeiten der Kategorisierung und der subjektiven Einschätzung von Operationellen Risiken bei der praktischen Umsetzung aufmerksam und warnen vor signifikanten Verzerrungen bei der VaR-Berechnung im Fall von Erhebungsfehlern.[769]

Aus Sicht des Autors gibt es für den Prozess der Festlegung von standardisierten Indikatoren, die Analyse der Daten und die Umsetzung der Erkenntnisse in mögliche Empfehlungen nur einen möglichen Akteur, der zumindest eine mitgestaltende und koordinierende Rolle einnehmen muss, soll das Projekt zum Erfolg führen: die Bank für Internationalen Zahlungsausgleich. Nimmt der Supervisory Review Process als zweite Säule von Basel II die wichtige Bedeutung ein, die in den Konsultationen herausgearbeitet wurde[770], ließe sich eine fortlaufende Datensammlung und Datenanalyse in dieses aufsichtliche Überprüfungsverfahren gemeinsam mit den Finanzinstituten hervorragend integrieren.

Der Supervisory Review Process ist in der zweiten Säule der Neuen Basler Eigenkapitalvereinbarung im Lauf der Konsultationen zunehmend gestärkt worden, während die dritte Säule, die Offenlegungspflichten, eher an Bedeutung verloren hat. Im Bereich Operationeller Risiken ist diese Entwicklung aus Sicht des Autors zu begrüßen. Dies gilt in besonderem Maße für Operationelle Risiken im elektronischen Zahlungsverkehr. Es ist vermutlich keinem der Akteure damit gedient, wenn potenzielle Risiken und realisierte Schadensfälle immer von neuem an die nicht fachspezifisch mit Vorkenntnissen belastete Öffentlichkeit dringen. Im schlechtesten Fall führen Ereignisse im Bereich Zahlungsverkehr zu so viel negativer Öffentlichkeitswirkung, dass der gesamte elektronische Zahlungsverkehr im Retail-Bereich betroffen wäre. Unter diesem Aspekt ist beispielsweise die im Frühsommer 2003 in Kalifornien erlassene Verordnung als kritisch zu betrachten, die Unternehmen mit Kunden in Kalifornien dazu zwingt, jeden Eindringling in ihr Firmennetz den Kunden zu melden. Es kann zwar mit einer erzieherischen Wirkung gerechnet werden, die Unternehmen werden alles tun, um eine solche Meldung zu vermeiden. Gleichzeitig kann aber ein negativer Effekt eintreten und das Unwohlsein der Konsumenten beim Nutzen von elektronischen Netzen so hoch werden lassen, dass die Akzeptanz dieser Netze zu sinken beginnt. Der französische Weg der Bankenaufsicht, im Zahlungsverkehr zunächst vertrauliche Warnungen auszusprechen und der betroffenen Firma die Möglichkeit zur Korrektur zu geben, bevor die öffentliche Stigmatisierung erfolgt, erscheint als aufsichtliches Instrument sehr viel zielgerichteter.[771]

Grundsätzlich bleibt gerade bei der dritten Säule bei der Offenlegung von Informationen die Arbeit der BIZ auf Empfehlungen und Anregungen beschränkt. Die BIZ betont den Spielraum, den die Aufsicht von nationalen Gesetzen und Verordnungen erhält und nutzen kann.[772] Die Ausführungen in den Basel II Entwürfen gehen auf Vorarbeiten der BIZ im Jahr 1998

[769] Vgl. Stocker et al. (2001), S. 684 f.
[770] Vgl. BIZ (2003c), S. 11 f.
[771] Vgl. Beau (2002).
[772] Vgl. BIZ (2003c), S. 13.

zurück, in denen einige Empfehlungen herausgearbeitet wurden, wie bestimmte Offenlegungspflichten auch im Bereich Operationeller Risiken die internen Bemühungen der Institute um besseres Risikomanagement in diesem Feld stärken könnten.[773]

Wird die Datensammlung und Datenanalyse für die Operationellen Risiken ebenso wie mögliche Schlussfolgerungen aus diesen Analysen, beispielsweise Empfehlungen der Aufsicht an die Institute, kooperativ zwischen Aufsicht und Instituten gelöst, gerät die zweite Säule mit dem SRP in den Vordergrund und die dritte Säule mit den Offenlegungspflichten verliert für die Beziehung zwischen Aufsicht und Finanzinstituten an Relevanz. Sie wird eher zur generellen Informationspolitik für die Öffentlichkeit genutzt, oder als gezieltes Sanktionierungsinstrument, und nicht zur Steuerung der aufsichtlich induzierten Anstrengungen der Finanzinstitute beim Management Operationeller Risiken benötigt.

5.3.3.3 Notwendige Erweiterungen der Datensätze

Im Rahmen der ersten Datenauswertungen im Zuge der QIS wird bei der BIZ der Wunsch nach einer Erweiterung der Datensätze zu Analysezwecken formuliert. Die BIZ schlägt bereits 2001 vor, die Finanzinstitute sollten interne Überprüfungen ihrer Schätzungen beginnen und weitere Indikatoren in den Datenbestand einbringen, unter anderem die Differenz erwarteter und tatsächlich realisierter Verlusthäufigkeiten und Verlusthöhen.[774] Ferner sollten die Institute selbst qualitative Faktoren auf ihre Eignung zur quantitativen Abschätzung Operationeller Risiken testen. Auch andere Autoren wie Beeck und Kaiser regen die Integration verschiedener Indikatoren wie Überstundenzahl, Fluktuationsrate und Systemausfallzeiten in die Modelle an.[775] Die BIZ kann sich in einem nächsten Schritt branchenweite Datenbanken vorstellen, deren Auswertung den beteiligten Finanzinstituten ein Benchmarking erlauben soll.

Anfang 2002 stellte die BIZ Überlegungen an, ob eine mögliche Ausweitung der Datenerhebung nicht im Rahmen der QIS erfolgen sollte und könnte.[776] Erste Vorschläge wurden zur Diskussion gestellt. Beispielsweise könnten die Orte, bei denen Schäden auftreten und der genaue Zeitpunkt eines Schadensereignisses mit erhoben werden.[777] Ab einer bestimmten Schadenshöhe wären ferner genauere Beschreibungen eventuell in Prosa und nicht standardisiert notwendig. Die BIZ regte zu einer Diskussion über diese Fragestellungen an, über mögliche Resultate wurde bis Sommer 2003 nicht (öffentlich verfügbar) berichtet.

Exemplarisch wird im folgenden für den Bereich Zahlungsverkehr eine Ausweitung der erhobenen Datensätze unter dem Aspekt der Datenanalyse zur Verbesserung des Managements Operationeller Risiken vorgeschlagen (siehe Tabelle 15).

Für den Zahlungsverkehr ergibt sich bereits bei der von der BIZ vorgegebenen Schadenshöhe von € 10.000, ab der Operationelle Risiken meldepflichtig sind, unter Umständen ein Problem.[778] Während im Großzahlungsverkehr einzelne Schadensfälle diese Schwelle in der Regel deutlich überschreiten, ist im Retail-Zahlungsverkehr der Einzel-Schaden oft geringer.

---

[773] Vgl. BIZ (1998e).
[774] Vgl. BIZ (2001l), S. 22.
[775] Beeck (2000), S. 648.
[776] Vgl. BIZ (2002a), S. 26.
[777] Bereits im Jahr 2000 hatten Autoren wie Beeck und Kaiser verschiedene Vorschläge über zu erfassende Informationen gemacht, allerdings gab es damals das Gerüst der QIS noch nicht. Vgl. Beeck (2000), S. 648 f.
[778] Der Autor geht an dieser Stelle davon aus, dass die BIZ sich mit der Schadenssumme auf das Einzelereignis bezieht. Ist die nicht der Fall, sind die Cluster-Schäden bereits berücksichtigt und nur nicht als solche von der BIZ gekennzeichnet.

Allerdings lassen sich bei diesen Schadensfällen oftmals Cluster bilden, die als Einzelschäden sofern sie in die Kategorie „high frequency – low impact“ fallen, in der Summe sehr viel höhere Schäden ergeben und die kausal auf eine Ursache zurückgeführt werden können, beispielsweise Ausspähmethoden der PIN. Werden die Einzelereignisse an dieser Stelle nicht erfasst und auf ihre Ursachen hin analysiert, kann eine bestimmte Schadensklasse nicht bankübergreifend beobachtet, und der potenzielle Schaden nicht effektiv gemindert werden.

Diese Schwierigkeit könnte mit der Konstruktion von Cluster-Schäden umgangen werden. Cluster-Schäden würde bedeuten, einzelne sich wiederholende Schäden vom gleichen Typ werden aufsummiert und in den Quantifizierungsansätzen und Datenreihen berücksichtigt – auch wenn jeder Einzelfall unter der Schwelle von € 10.000 liegt. Da im Zahlungsverkehr die Öffentlichwirksamkeit von kumulierten Schäden ein Reputationsproblem darstellt, wäre es aus Sicht des Autors legitim, in diesem Bereich eine Sonderregelung für die Datenerhebung durchzusetzen – auch wenn Reputationsrisiken ausdrücklich keine Operationellen Risiken im Sinne der BIZ-Definition sind.

Die Schadenshöhe ist bei Vergleichen einzelner Institute untereinander ohnehin eine kritische Größe. Werden die Schadensmeldungen nicht nach der Größe des den Schaden meldenden Instituts skaliert, kann ein Schaden, der bei einer internationalen Großbank kaum in den Büchern auftaucht, die Existenz eines kleineren nationalen Instituts gefährden.[779] Dieser Aspekt ist für die institutsinterne Priorisierung einzelner Aktionen im Rahmen des Managements Operationeller Risiken von Bedeutung.

Für die Analyse von Schadensfällen und die mögliche Mustererkennung von beispielsweise Betrugsfällen, vor denen andere Finanzinstitute gewarnt werden sollen, ist die reine Schadenshöhe von untergeordneter Bedeutung. Hier spielt die potenzielle Schadenshöhe im Fall erfolgreicher Angriffe für die Einschätzung des notwendigen Handlungsbedarfs eine wesentlichere Rolle. Ist die Eintrittswahrscheinlichkeit einer theoretisch denkbaren aber noch nicht eingetretenen Angriffsvariante oder eines technischen Schadensfalls nicht einschätzbar, muss in nächster Näherung versucht werden, den Aufwand zur Behebung dieses Problems zu beziffern. Dann muss eine institutsinterne Einschätzung der Dringlichkeit der Maßnahme erfolgen. Es bietet sich an, gegebenenfalls Indikatoren festzulegen, bei deren Eintreten oder Erreichen, das jeweilige Institut Gegenmaßnahmen erreicht. Beispielsweise kann bis zum ersten erfolgreichen Angriff auf eine Verschlüsselungsmethode diese verwendet werden, allerdings sollten für den Ernstfall zeitnah zu realisierende Alternativen existieren – ansonsten droht die Gefahr, dass beispielsweise die Kreditkarteninstitute bei dem in Abschnitt 5.3.2.1.1 beschriebenen Kreditkartenbetrugsfall durch Kompromittierung ihres verwendeten Verschlüsselungsalgorithmus kaum noch in einem realistischen Zeitfenster und zu überschaubaren Kosten begegnen können.

Aus Sicht des Autors bietet es sich an, sofern die Klassifizierung hinreichend systematisch erfolgt, und die Aufnahme der Daten in eine Schadensdatenbank einfach erfolgen kann, in einem ersten Schritt eher zu viele Einzelinformationen zu einem Schadensfall zu sammeln. Erst mit fortschreitender Erfahrung bei der Auswertung der Schäden, bei der Mustererkennung und der Festlegung von Indikatoren kann die Auswahl der relevanten Datenpunkte wirkungsvoll getroffen werden.

Für eine weitgehend überschneidungsfreie Ausweitung der Datenerhebung im Bereich Operationeller Risiken bietet sich der erweiterte Sicherheitsbegriff des Schalenmodells an.

[779] Vgl. Peter (2000), S. 668.

Ein wesentlicher Vorteil des Schalenmodells ist die Trennung der technisch orientierten und der organisatorisch basierten Ursachen, die einem Schadensfall zugrunde liegen. Ein weiterer Vorteil liegt in der Möglichkeit, die Kategorisierung der BIZ nahtlos fortzusetzen, ohne die bestehende Einteilung in Frage zu stellen.

Die äußere gesellschaftliche Ebene der Sicherheit im Schalenmodell ist für die vorliegende Betrachtung nicht von Bedeutung, da sich die Ursachen für die Verletzung dieser Ebene durch die darunterliegenden erklären lassen. Somit bleiben drei relevante Kategorien übrig (siehe Tabelle 16):

1. Die Ebene der IT-Sicherheit, die technische Fragestellungen behandelt.
2. Die technisch-organisatorische Ebene, bei der technische Fragestellungen zwar von Belang sind, jedoch organisatorisch korrekt gelöst werden müssen, um Sicherheit zu gewährleisten.
3. Die rechtlich-ökonomische Ebene, bei der durch juristische Schwierigkeiten oder durch Ausnutzen bestimmter Regelungen, für die Finanzinstitute nachteilige Schäden entstehen können.

Die technische Ebene kann weiter aufgeteilt werden, orientiert an den informationstechnologischen Kategorien der Sicherheit. Somit könnten Angriffe und Probleme im Bereich technischer Sicherheit auf die Aspekte Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit zurückgeführt werden.

Die Auswertung der LDCE hat eine auffällige Häufung von Schadensfällen im Bereich interner und externer Betrug sowie im Bereich der Transaktions- und Prozessfehler ergeben. Insofern erscheint es auf der Suche nach Ursachen für Betrug legitim, bei diesen Fällen die Art der Angriffe und die vermutlichen – oder bereits ermittelten – Angreifer mit zu erfassen. Bei Angriffen ist die Frage von Bedeutung, um welche Art von Angriff es sich handelt. Erst anhand einer Antwort auf diese Frage kann die Prioriät von Gegenmaßnahmen und die Art der Gegenmaßnahmen sinnvoll festgelegt werden. Systeme sind aus unterschiedlichen Gründen Angriffen ausgesetzt. Dabei ist einerseits zwischen der Art des Angriffs und andererseits dem Typ des Angreifers zu unterscheiden. Schneier unterscheidet vier grundsätzliche Arten von Attacken[780]. Die kursiv gedruckten Fälle sind für den Zahlungsverkehr von besonderer Bedeutung:

Kriminelle Attacken mit diversen Ausprägungen:
- *Betrug,*
- *Scams* (Geld einkassieren und ohne Gegenleistung verschwinden) – ein typisches Delikt im Bereich Online-Auktionen,
- zerstörerische Aktionen,
- Diebstahl geistigen Eigentums,
- *Identitätsdiebstahl* (z. B. Eindringen in PayPal-Account, wenn Passwort ausgespäht),
- Markendiebstahl,
- *Verletzung der Privatsphäre* (z. B. Ausspähen von Kontoinformationen)
- *Angriffe, die das existierende Rechtssystem ausnutzen*:
  z. B. der Missbrauch einer Kreditkarte oder Kontonummer (im Lastschriftverfahren) und anschließendes Leugnen, diese benutzt zu haben,

[780] Vgl. Schneier (2000), S. 23 ff.

- *Angriffe, die dazu dienen Aufmerksamkeit zu erzeugen*: z. B. Veränderung von Webpages
- Distributed Denial of Service-Attacken
- Angriffe, die durch Sabotage wirtschaftlichen Schaden erzeugen wollen.

Parameter	Ausprägungen	Erläuterung
Cluster-Schäden	Aufsummierung ähnlicher Fälle, um über den Schwellenwert zur Schadenserfassung zu kommen	Im Zahlungsverkehr gehen sonst kleinere Schadensfälle, die häufig auftreten unter
Skalierungsfaktor für Operationellen Schadensfall	Faktor, der Institutsgröße je nach Fall berücksichtigt	Sonst kommt es zu Verzerrungen bei der Priorisierung von Maßnahmen
Schadenspotenzial	gering – mittel – hoch	Schwierigkeit besteht in quantitativer Aussage. Einschätzung ist subjektiv.
Erweiterter Sicherheitsbegriff	technisch, technisch-organisatorisch, juristisch-ökonomisch	Erleichert die Analysephase und Mustererkennung erheblich
Technische Ebene – Komponenten	Verfügbarkeit, Vertraulichkeit, Integrität,Zurechenbarkeit	Weitere Aufteilung der technischen Ebene zur Analyse
Angriffe	Betrug, Aufmerksamkeit, Sabotage, Ausnutzen Rechtssystem	Wichtiger Aspekt zur Gewichtung der Maßnahmen
Angreifertypen	Hacker oder Cracker, Kriminelle externe Einzelgänger, Kriminelle Insider/Frustrierte Mitarbeiter/Gelegenheitsdiebe, Industrielle Spionage, Presse, organisierte Kriminalität, öffentliche Stellen, Terrorgruppen, Kombinationen	Wichtiger Aspekt zur Gewichtung und Aufwand der jeweiligen Maßnahmen
Verwendung bestimmter Komponenten	Typ Software/Hardware	Bei systembedingten Problemen können Reaktionszeiten deutlich verkürzt werden.
Öffentlichkeitswirkung	niedrig – mittel – hoch	Bedeutung für Public Relations aber auch Aufsicht
Reproduzierbarkeit	niedrig – mittel – hoch	Für Analyse und Mustererkennung
Geschätzte Kosten der „Beseitigung“/Tatsächliche Kosten	Zahl	Falls erhebbar von großer Bedeutung für Kosten-Nutzen-Analyse
Land	Wo hat Ereignis stattgefunden?	Berücksichtigung möglicher Länderspezifika bei Analyse

Tabelle 15: Vorschlag für die Erweiterung der Parameter bei der Erfassung Operationeller Risiken

Es sind zwar Kombinationen denkbar, bei denen beispielsweise nach erfolgreichem technischen Angriff Lücken in den Allgemeinen Geschäftsbedingungen ausgenutzt werden. In

diesem Fall hilft die Kausalitätsbetrachtung. Der auslösende Faktor ist für die Kategorisierung maßgeblich, im Beispiel wäre die technische Ebene betroffen.

Ebene der Sicherheit	Beispiel für Schadensfall
technisch	Auslesen der PIN bei Kreditkarten und anschließender Kartenmissbrauch
technisch-organisatorisch	Zwei Innentäter, die eine technische Autorisierung durch Kooperation bewältigen
juristisch-ökonomisch	Betrug durch Rücklastschrift, falls Authentifizierung nicht mit rechtsverbindlicher Unterschrift realisiert wurde

Tabelle 16: Kategorisierung von Operationellen Risiken und beispielhafte Schadensfälle im Zahlungsverkehr

Für die Einschätzung der Bedrohungslage ist der Frage nachzugehen, wer die Angreifer in einem bestimmten Fall sind. Die Frage wird unter Umständen beim Eintreten eines Schadensfalls nicht sofort zu beantworten sein. Gleichwohl gibt es gewisse Indikatoren, die als Anhaltspunkt dienen können. Die Datenbank kann zur Not auch im Nachhinein um eine solche Information ergänzt werden.

Die Gruppe der Gegenspieler von Sicherheitsbestrebungen ist in ihrer Heterogenität äußerst unterschiedlich bezüglich ihrer Ziele, ihrer eingesetzten Ressourcen und ihrem Systemzugang zum Erreichen dieser Ziele. Es lassen sich unterscheiden:[781]

- Hacker oder Cracker (Das Interesse an finanzieller Ausbeute ist zumeist gering. Motivation ist die Reputation, die man durch einen erfolgreichen Angriff in der Szene erwirbt)
- Kriminelle externe Einzelgänger
- Kriminelle Insider/Frustrierte Mitarbeiter/Gelegenheitsdiebe (haben zufällig eine lukrative Lücke im System entdeckt)
- Industrielle Spionage
- Presse (meist mit publizitätsträchtigen Ergebnissen ein Reputationsproblem schaffend, direkte finanzielle Schäden gering)
- Organisierte Kriminalität
- Öffentliche Stellen: Polizei/Verfassungsschutz/Geheimdienste (in westlichen Ländern vermutlich von geringster Bedeutung)
- Terrorgruppen
- Kombinationen dieser Angreifer, beispielsweise Insider, die mit kriminellen Vereinigungen kooperieren, oder zur Zusammenarbeit erpresst werden.

Die verschiedenen Tätergruppen unterscheiden sich nicht nur in den Tatmotiven, sondern auch in der Gefährlichkeit für die angegriffene Branche und Institution erheblich. Hacker und Cracker verfügen in der Regel über ausgewiesene Netzwerke und kommunizieren bei erfolgreichen Angriffen die Angriffsmöglichkeiten. Eine Gefahr kann entstehen, wenn diese Angriffsmöglichkeiten von kriminellen Tätern, die auf finanziellen Erfolg zielen, ausgenutzt werden können. Dabei fehlt bei den Einzeltätern, die monetären Nutzen aus ihren Aktionen ziehen wollen, in der Regel der logistische Background, um elektronisch generierte Summen auch tatsächlich unverdächtig in Bargeld umzuwandeln. Die zunehmend strengeren Bestimmungen gegen Geldwäsche aber auch die internationalen Überwachungsmaßnahmen gegen Terror erschweren diesen Schritt mehr und mehr. Interne Angreifer und Gelegenheitsdiebe,

[781] Vgl. Schneier (2000), S. 42 ff.

die eine eher zufällig entdeckte Lücke systematisch ausnutzen, verursachen je nach Zeithorizont, in dem sie ihre Tat begehen, zwar teilweise erhebliche Schäden. Diese sind aber in der Regel überschaubar und werden durch ein funktionierendes Management Operationeller Risiken aufgedeckt. Die Gefahr, dass beispielsweise in anderen Instituten Kriminelle die gleiche Schwachstelle ausnutzen, ist zwar theoretisch gegeben, aber ein gezielter Informationsfluss existiert nicht. Es steht zu vermuten, dass einige der von dieser Tätergruppe ausgenutzten Schwachstellen bei einer Schadensanalyse auch der Transaktions- und Prozessfehler im Rahmen des Managements Operationeller Risiken entdeckt und beseitigt werden können. Während industrielle Spionage zwar ein immer häufigeres Delikt zu werden scheint, ist der Zahlungsverkehr davon zunächst nicht betroffen. Ein größeres Problem stellen publizitätswirksame Angriffe auf den Zahlungsverkehr in seinen Ausprägungen dar. In Deutschland ist das eBanking aber auch der HBCI-Standard (Homebanking Computer Interface) durch Fachjournalisten und TV-Beiträge immer wieder in Verruf geraten – ein Reputationsproblem mit schwierig zu prognostizierendem Schadenspotenzial. Auch hier kann jedoch erwartet werden, dass ein gezielt bei Betrugsfällen und Prozessfehlern angreifendes Risikomanagement die Wahrscheinlichkeit von erfolgreichen journalistischen Angriffen zumindest erheblich reduziert.

Die potenzielle Schadenshöhe ist im Bereich Zahlungsverkehr mit hoher Wahrscheinlichkeit bei kriminellen Vereinigungen, die schlimmstenfalls mit Insidern kooperieren, am höchsten. Hier kommt es zur unter Umständen gefährlichen Mischung aus Systemkenntnissen, technischem Wissen und internationalem Netzwerk. Ein Beispiel sind die international organisierten Banden, die Kreditkarten (und zunehmend auch Debitkarten) fälschen (Totalfälschung) und im Ausland einsetzen. Sie generieren hohe Schäden. Das Entdeckung-Risiko ist für die Kriminellen bislang eher gering.[782] Terrorgruppen und öffentliche Stellen stellen kein spezifisches Problem für den Zahlungsverkehr dar. Durch die verstärkten Maßnahmen zur Terrorbekämpfung dürfte es für Terrornetzwerke zumindest schwieriger werden, Gelder weltweit zu transferieren. Ein Interesse derartiger Gruppen, den Zahlungsverkehr als solchen anzugreifen, ist nicht dokumentiert.

Es lassen sich für den Fall von Prozess- und Transaktionsfehlern weitere Parameter denken, die in einer Schadensfalldatenbank erhoben werden sollten. Relevante Fragen zielen beispielsweise auf die Art der eingesetzten Soft- und Hardware. Gab es Schnittstellenprobleme? Ein typisches Problem im Zahlungsverkehr können bei Lastschriften die Probleme mit fehlerhaften Kontonummern und Bankleitzahlen sein, die, ohne dass eine betrügerische Absicht vorliegt, zu einer Rücklastschrift führen.

Ein weiterer Parameter, der aus Sicht der Finanzinstitute und für die Aufsicht von Bedeutung ist, ist der potenzielle Grad an Öffentlichkeitswirkung eines Schadensfalls. Hohe Priorität bei der Schadensbekämpfung hätten demnach Fälle, die aufgrund einer Schädigung von vielen Kunden schnell eine hohe Publizität erreichen. Auch Schadensfälle, die die Sicherheit der von den Finanzinstituten eingesetzten Verfahren in Zweifel ziehen, fallen in diese Kategorie. Interne Ereignisse hingegen können zwar empfindliche Schäden bewirken, sind jedoch „unauffälliger“ und können mit anderem Zeithorizont bearbeitet werden. Sollte es bei Eintritt und Erfassung eines bestimmten Schadensfalls bereits möglich sein, eine solche Aussage zu treffen, wäre die Frage nach der potenziellen Reproduzierbarkeit eines Schadensereignisses von Belang. Kann diese Frage mit ja beantwortet werden, steigt die Priorität, eine Gegenmaßnahme zu finden, deutlich gegenüber einem Einzelfallereignis.

[782] Vgl. Preuß (2002).

Für die Legitimation der erfolgenden Maßnahmen, und um ein Gespür für die Kosten-Nutzen-Relation zu bekommen, wäre es wünschenswert, bei Schadensfällen neben den durch den Fall entstehenden Schadenssummen auch die geschätzten Kosten für die Beseitigung des Risikos anzugeben. Zwei Möglichkeiten wären denkbar. Erstens eine ex ante Schätzung, die angibt, mit Kosten in welcher Größenordnung gerechnet werden kann, um einen ähnlichen Schadensfall in Zukunft zu vermeiden, zweitens eine ex post Größe, die die tatsächlich aufgewendeten Summen, sofern diese direkt erfasst werden können, angibt. Allerdings kommt es bei dieser Position in besonderem Maße wieder zu Verzerrungen durch die unterschiedliche Größenordnung der beteiligten Finanzinstitute. Wird über eine Erhebung der Kosten nachgedacht, können für die Auswertung mit Einschränkungen nur Institute der selben Kategorie miteinander verglichen werden. Oder es müssten Skalierungsfaktoren eingeführt werden, die ohnehin bei allen Fragen der Datenaggregation relevant werden.

Eine ähnliche Argumentation gilt für länderspezifische Operationelle Risiken, die beispielsweise an die Verwendung einer bestimmten Infrastruktur gekoppelt sind, oder durch spezifische juristische Ausprägungen bedingt werden. In der Folge muss der Parameter „Land, in dem der Schadensfall aufgetreten ist“ mit in die Datenerhebung integriert werden.

5.3.3.4 Vorschlag für ein kooperatives Modell für das Management Operationeller Risiken

Bei der Auswertung der gewonnenen Daten gilt es eine Schwierigkeit zu vermeiden, der die Kreditbewertungsmodelle im Laufe ihrer Entwicklung begegnet sind. Wurden dort zunächst die ökonomischen Bestimmungsfaktoren herausgearbeitet, die zu mangelnder Kreditwürdigkeit eines Kreditnehmers beitragen, geriet die nächste Stufe der Analysen zur rein statistischen Datenaufbereitung, ohne weiterhin die ökonomischen Zusammenhänge zu berücksichtigen.[783]

Es lässt sich eine Analogie zu der Quantifizierung Operationeller Risiken erkennen, die im Hinblick auf die Ursachen und mögliche Bestimmungsfaktoren deutlich weiter gestreut sind als beispielsweise Marktrisiken. Die QIS Analysen sind auf die statistischen Verfahren zur Aufbereitung der Daten und die Zulässigkeit einzelner Verfahren bei bankinternen Ansätzen konzentriert und haben die eigentliche Ursachenforschung, die in der Vermeidung Operationeller Risiken resultieren kann, den Finanzinstituten überlassen – bisher mit dem Resultat, dass wesentliche Ergänzungen der Datensätze bei der Erhebungsphase noch nicht stattgefunden haben.

Die aufwändigen Prozessanalysen, die für jeden Prozess und jedes Produkt individuell durchgeführt werden müssen, sind zumindest in den nächsten Jahren bei aller Konzentration auf Risikosteuerung und -management nur für ausgewählte Bereiche finanziell zu bewältigen. Für den Geschäftsprozess „Überweisungsauftrag“ hat Simon die Komplexität einer Prozessanalyse anschaulich gemacht.[784] Dabei wird zunächst lediglich der beleghafte finanzinstitutsinterne Vorgang von der Eingabe des Beleggutes in Terminals bis zur Erstellung von Tagesauszügen untersucht. Es werden alle Schritte einzeln erfasst, auf Fehlerquellen und Angriffsmöglichkeiten untersucht, Fehlerindikatoren gesucht und eine erste Auswertung versucht. Im Ergebnis wird eine Matrix ausgefüllt, die in den Zeilen die Prozessschritte abbildet und in den Spalten Irrtums-, Modell- und Betriebskostenfehler verschiedener Art aufträgt. Mit Scoring-Verfahren kann im Anschluss versucht werden, eine Priorisierung der erforderlichen Maßnahmen zu erreichen.

[783] Vgl. Rudolph (2000), S. 30 f.
[784] Vgl. Simon (2002), S. 134 ff.

Wird bei einer solchen Prozessanalyse der gesamte Prozess von der Initiierung beim Kaufvorgang und der Rechnungsstellung bis zur Warenübergabe untersucht, und damit die außerhalb der direkten Kontrolle der Finanzinstitute liegenden Vorgänge, nimmt die Komplexität der Analyse erheblich zu. Der Versuch, für solche Prozesse formale Methoden zu verwenden, ist – ohne viele einschränkende Annahmen – schwierig bis unmöglich.

Ein Beispiel für die notwendigen Anstrengungen bei formalen Ansätzen bieten die Electronic Money Security Objectives, die orientiert an den Common Criteria[785] formal die Sicherheitsziele für – noch kaum am Markt vorhandenes – elektronisches Geld definieren.[786] Dieser Schritt ist jedoch der verhältnismäßig leichtere. Schwierig wird dann die konkrete Umsetzung dieser Ziele auf Prozessebene in komplexem Marktumfeld mit unbestimmbaren Sicherheitskomponenten, beispielsweise dem Computer, den der Konsument verwendet. Diese Schwierigkeit mag ein Grund dafür sein, dass zwar im Finanzsektor einige Protection Profiles orientiert an bereits erarbeiteten Security Objectives gemäß Common Criteria existieren, beispielsweise im Sparkkassensektor das „Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleister“[787], allerdings keine darauf aufgebauten und dokumentierten durch die gesamte Organisation mit Außenbezügen evaluierten Produkte und Prozesse existieren. Selbst die Organisation SWIFT, ein Vorreiter bei der Zertifizierung gemäß ISO/IEC 17799 in der Finanzwelt, hat keine formal höheren Zertifizierungen nach den Common Criteria für Gesamtprozesse absolviert.

Die Finanzbranche steht der Idee, formal geprüfte Soft- und Hardware einzusetzen, durchaus positiv gegenüber.[788] Allerdings stößt die Branche auf die gleichen Probleme, die auch Regierungen beim geforderten Einsatz evaluierter Produkte haben: Es gibt noch sehr wenige Produkte, die in ausreichend hohen Sicherheitsstufen evaluiert und zertifiziert sind. So listet die US-Regierungsinitiative, die für sicherheitskritische Einsätze CC-evaluierte Produkte fordert, lediglich 93 solcher Produkte auf, die Tendenz ist aufgrund der Regierungsnachfrage allerdings steigend. Zusätzlich sind die Kosten für die Evaluation beträchtlich: „EAL7 is the highest rating, but any rating above EAL4 is said to be extremely hard to achieve and requires additional government-lab review.“[789] Bereits für EAL4 lautet die Aussage für Systeme, die im Einsatz sind: “…the highest level at which it is likely to be economically feasible to retrofit an existing application”.[790] Beispielsweise liegen die Kosten für eine EAL4-Evaluation für ein Intrusion-Detection-System bei bis zu US-$ 400.000 – bei einer Evaluationsdauer von über einem Jahr und Engpässen bei geeigneten Test-Laboratorien.[791]

Die Kosten/Nutzen-Relation ist der begrenzende Faktor. Es erscheint sinnvoll, eine Datenanalyse der Operationellen Risiken als ersten Indikator zu verwenden, in welchen Bereichen weitergehende Prozessbetrachtungen notwendig sind. Wird ein Warnsystem installiert, das beispielsweise nach der Analyse von Schadensfällen die Finanzinstitute über Schadensfallmuster, Angriffsmuster oder ähnliches informiert, kann dieses System ebenso verwendet werden, um Informationen über potenzielle Angriffe, die in der Datenbank noch keinen Niederschlag gefunden haben, an die Institute zu übermitteln.

[785] Vgl. ISO 15408-1(1999) und ISO 15408-2(1999).
[786] Vgl. EZB (2003b).
[787] Vgl. SIZ (2000).
[788] Vgl. o.V. (2003c).
[789] o.V. (2003c), S. 2. EAL: Evaluation Assurance Level.
[790] o.V. (2003c), S. 3.
[791] Vgl. o.V. (2003), S. 4.

An dieser Stelle liegt der mögliche Nutzen einer supranationalen mit der Aufsicht kooperierenden oder bei ihr angesiedelten Institution beispielsweise im Rahmen der Basler BIZ, die mit der Sammlung und Analyse der Daten zu Operationellen Risiken in Finanzinstituten beauftragt ist. Solange sich eine umfassende Prozessanalyse für alle Bereiche nicht rechnen lässt, versuchen die einzelnen Finanzinstitute auf Verdacht, oder aufgrund eigener bereits realisierter Schadensfälle, Prozessanalysen gezielt einzusetzen. Eine Institution, die Datensammlung und –analyse betreibt, kann basierend auf dem weitergehenden Datenmaterial vorhandene Schadensfälle institutsübergreifender Art erkennen, erkannte Muster bei realisierten Schadensfällen als Frühwarnung herausgeben und vor vermuteten Schwachstellen und Gefahren warnen, die noch nicht notwendigerweise zu Schadensfällen geführt haben.

Die Möglichkeit einer supranationalen Institution unter Beteiligung der BIZ bietet die Chance, die mit den QIS und LDCE begonnene Standardisierung bei der Erhebungsphase Operationeller Risiken weiter fortzusetzen. Die Weiterentwicklung und Festlegung zusätzlicher Datenfelder wie im vorigen Abschnitt beschrieben, kann dann effizient von einer Stelle koordinierend ausgehen, unter Beteiligung aller interessierten Akteure.

Die Analyse der Daten kann ebenfalls kooperativ abgewickelt werden auf dem jeweils verfügbaren Wissen zum Thema Risikomanagement basierend. Um eine Übergewichtung einzelner Akteure zu vermeiden, beispielsweise aufsichtliche Belange in den Vordergrund zu drängen, kann ein Prozedere bei der Abgabe von Empfehlungen des Gremiums erarbeitet werden. Beispielhaft ist an eine Stimmrechtsvergabe eines Expertengremiums zu denken, bei dem Vertreter der Finanzinstitute und der Aufsicht gemäß einem festgelegten Schlüssel Stimmrechte erhalten. Sollen von diesem Gremium Warnungen, Umsetzungsempfehlungen oder aufsichtliche Anordnungen herausgegeben werden, kann das Gremium per Abstimmung über die Relevanz bestimmter Einschätzungen zu einem neutralen Ergebnis kommen.

Es existieren verschiedene Möglichkeiten, mit welchen Kompetenzen eine solche Institution – ein Zentrum zur Erhebung und Analyse Operationeller Risiken im Finanzsektor (ein möglicher, die Aufgabenbereiche charakterisierender, Namensvorschlag wäre „Operational Risk Emergency and Analysis Centre“) – ausgestattet werden kann. Zentrale Fragen wären unter anderem, wie die Schnittstellen zu bereits vorhandenen Datenbankkonsortien aussehen könnten, ob die Analyse dezentral geschehen kann und das Zentrum anschließend die Aufgabe der Gewichtung übernimmt und die Frage nach der Verwendung einer bestimmten Softwarelösung oder lediglich die Schnittstellenspezifikation. Aus Sicht des Autors wäre eine zentrale Datensammlung und eventuell sogar Analyse für alle Beteiligten aufgrund der maximalen Verfügbarkeit aller Informationen vorteilhaft. Dieser Ansatz schließt nicht aus, dass ein solchermaßen aufgestelltes Zentrum, die gesammelten Daten auch an separate Institute und deren Analysezentrum weitergibt oder zur Verfügung stellt. Treten die an der Analyse beteiligten Akteure in Dialog, besteht die Möglichkeit die Qualität verschiedener Verfahren im Vergleich zu diskutieren.

Es existiert bereits eine Vielfalt von Initiativen, die Datenbanken zu verschiedenen Risiken aufbauen, beispielsweise die von Totem Market Valuations mit PriceWaterhouseCoopers betriebene TOTEM Datenbank mit Marktrisikodaten.[792] In Analogie zum Erfolg solcher Ansätze bemühen sich in jüngster Zeit verschiedene Initiativen um den Aufbau von Datenbanken zu Operationellen Risiken[793], beispielsweise die British Bankers' Association[794] und

[792] Vgl. Stickelmann (2002), S. 7 ff.
[793] Vgl. Jörg (2002), S. 52 f.
[794] Vgl. www.bba.uk

die Global Association of Risk Professionals (GARP)[795]. Die British Bankers' Association hat die Federführung bei der Global Operational Loss Database (GOLD). GARP wiederum beauftragte das Unternehmen NetRisk, Entwickler von Software zur Risikosteuerung, die Datenbank Multinational Operational Risk Exchange (MORE)[796] aufzubauen und zu pflegen. In Zürich befindet sich die Operational Riskdata eXchange (ORX), ein weiteres Datenkonsortium, in welchem die jeweiligen Mitgliedsbanken ihre Verlustdaten sammeln.

Die Schwierigkeiten beim Aufbau einer einheitlichen Datenbank für Operationelle Risiken sind bereits bei einem konsolidierten Datenbankbetreiber, dem erwähnten Zentrum zur Erhebung und Analyse Operationeller Risiken im Finanzsektor, nicht zu vernachlässigen. Neben der Einigung auf einheitliche Merkmale müssen unter anderem Validitätstests für die Daten entwickelt und einheitliche Standards für die Datenerhebung bei den Instituten festgelegt werden. Dabei gilt es Fragen der Vertraulichkeit und Anonymität der Daten ebenso zu gewährleisten wie die Datenkonsistenz zu sichern. Nicht zuletzt stellt sich die Frage, ob die institutsinterne Datenerfassung zum Gegenstand aufsichtlicher Überprüfung, von internen oder externen Audits werden sollte. Im Laufe der Auswertung zunehmender Datenmengen wird sich zudem zeigen müssen, inwieweit länderspezifische Besonderheiten berücksichtigt werden müssen. Beispielsweise können insbesondere juristische Konstruktionen in einem Land A ausgenutzt werden, die in Land B anders formuliert sind oder nicht existieren. An dieser Stelle muss dann das Zentrum die gewünschte Interpretation der Daten und die zielgerichtete Informationspolitik übernehmen.

Die Datensammlung in Datenkonsortien ermöglicht auf der einen Seite zwar eine vielfältigere Suche nach verschiedenen Ansätzen, auf der anderen Seite gehen bei fehlender Kooperation unter den Konsortien Dateninformationen verloren. Ungelöst bleibt vorerst die Kompatibilität der Daten, wenn nicht ein übergeordnetes Gremium entsprechende Kriterien erarbeitet.

Für die Durchführung der Erhebung und das Feedback einer erfolgten Datenanalyse ist ein softwaregestützter Ansatz zwingend. Es gibt bereits verschiedene Verfahren, die in der Praxis eingesetzt werden, wie z. B. das vom Bundesverband Öffentlicher Banken Deutschlands mitentwickelte Operational Risk Center oder die Modelle von PriceWaterhouseCoopers. Sie bieten eine an den Vorgaben von Basel II orientierte Gesamtlösung zur Steuerung Operationeller Risiken.[797] Im Zentrum der bisher eingesetzten Verfahren steht die Möglichkeit a) der Quantifizierung der mit verschiedenen Methoden erfassten Risiken b) die Gewichtung dieser Risiken mit Scoring-Ansätzen und c) die daran orientierte Steuerung oder Allokation von Risikokapital für Operationelle Risiken. Die eigentliche Analysephase und Ausarbeitung von Empfehlungen, wie einzelnen Operationellen Risiken begegnet werden kann, ist (noch) nicht Gegenstand dieser Module.

Vorteilhaft wäre zur einheitlichen Datenerhebung ein Software-Modul, das auf der Baumstruktur der BIZ-Vorgaben basiert. Diese ist in Abbildung 30: Entscheidungsbaum: Klassifikation der Schadensfälle nach Basel II" bereits etabliert und verhindert weitgehend die Fehlkategorisierung von aufgetretenen Operationellen Schadensfällen. Notwendig für eine substanzielle Datenanalyse wäre die in Tabelle 15 entwickelte Erweiterung der Erhebungsphase, die sich im Wesentlichen an die Klassifikationsphase gemäß Entscheidungsbaum in Abbildung 30 anschließt. Dort werden aufgetretene Schadensfälle sieben vorgegebenen Schadensklassen zugeordnet. Lediglich bei der Behandlung von Cluster-Schäden müsste der Entscheidungsbaum leicht modifiziert werden. Statt der Frage, ob die Summe der Schäden

[795] Vgl. www.garp.com.
[796] Vgl. www.moreexchange.com.
[797] Vgl. Interexa (2002) und Stocker et al. (2001).

über dem Schwellenwert liegt, müsste dezidiert nach Clusterschäden gefragt werden. Die Frage, ob ein Skalierfaktor angewendet werden sollte, gehört zur detaillierten Abfrage des Einzel-Schadensereignisses und kann nach der Klassifikationsphase geklärt werden. Die Bestimmung der Höhe eines solchen Skalierfaktors ist nicht Gegenstand der an die Klassifikation anschließenden erweiterten Erhebungsphase. Zusätzlich besteht die Möglichkeit, für bestimmte Geschäftsbereiche unterschiedliche Faktoren anzuwenden, beispielsweise im Zahlungsverkehr andere als im Firmenkundengeschäft.

Die erweiterte Abfrage neuer Parameter ersetzt nicht die Auswertung. Durch die Strukturierung, beispielsweise nach Angriffsart oder Angreifertypen kann einerseits die Analyse zielgerichteter vorgenommen werden, andererseits eine Priorisierung einzelner Ereignisse und notwendiger Folgemaßnahmen leichter erfolgen.

Ein weiteres Problem muss gelöst werden: Handelt es sich um komplexe, kaskadierend verlaufende Schadensereignisse, werden z. B. in verschiedenen Geschäftsbereichen Schadenssummen durch einen Vorfall gemeldet, muss die Stelle eindeutig bestimmt werden, die den Schadensfall in die Datenbank einträgt. Ansonsten sind Doppelzählungen unvermeidlich. Es erscheint sinnvoll die quantitative Bestimmung eines Schadensfalles im Controlling anzusiedeln, ansonsten können subjektive Schätzungen aus unterschiedlichen Abteilungen die Validität der Datensammlung stark negativ beeinflussen. Letztlich wird die einheitliche Bestimmung monetärer Schätzgrößen einer eigenen institutsübergreifenden Systematik bedürfen. Für die Entwicklung einer solchen Systematik ist der dargestellte kooperative Ansatz ebenfalls zielführend.

6 Institutionelle und regulatorische Rahmenbedingungen im Hinblick auf sicheren elektronischen Zahlungsverkehr

6.1 Entwicklungslinien im Zahlungsverkehr und Implikationen für die Regulierung

Die Regulierung der Zahlungssysteme durch die unterschiedlichen Akteure – internationale Organisationen, europäische und nationale Gesetzgeber, Zentralbanken, private Organisationen etc. – spielt sich in einem komplexen und dynamischen Marktumfeld ab. Der Zahlungsverkehr entwickelt sich als Geschäftsfeld mit volkswirtschaftlicher Querschnittsfunktion in einer Umgebung die Artopoeus zutreffend charakterisiert:[798] „Die mit der ständig schwellenden Flut neuer Finanzprodukte einhergehende größere Volatilität der Märkte, die zunehmende Internationalisierung des gesamten Finanzdienstleistungsbereichs, die ins Gigantische wachsende Größe der internationalen Bankkonzerne und die steigende Ansteckungsgefahr, die sich aus der engen internationalen Verflechtung der Märkte und der Banken ergibt, erhöhen tendenziell das systemische Risiko." Wurde in Kapitel 4 bereits auf die strategische Positionierung einzelner Player eingegangen, erfolgt an dieser Stelle ein kurzer Abriss über die Entwicklungsrichtungen des Zahlungsverkehrs und mögliche Folgen für die Regulierung.

Die Nachrichtenübermittlung im internationalen Zahlungsverkehr erfolgt vielfach über das SWIFT-Netz. Im SWIFT-Geschäftsbericht 2002 lautet die Markteinschätzung des Zahlungsverkehrs: „The conference (SIBOS 2002 in Genf (Anmerkung d. V.)) revealed an industry facing unprecedented change."[799] Diese Aussage trifft für den europäischen Zahlungsverkehr in besonderem Maße zu, da die Integration des Euro-Raumes die Infrastruktur der Zahlungssysteme betroffen hat und weiter betrifft. Die Single Euro Payments Area (SEPA) hat zu einer deutlichen Konsolidierung im Segment der Großbetragszahlungssysteme geführt, TARGET ist als dezentral operierendes Brutto-Echtzeit-Zahlungssystem unter Regie der EZB erfolgreich gestartet. Mit TARGET2, dessen Konzeption aktuell im Eurosystem diskutiert wird, soll die Konsolidierung der vor allem aus politischen Gründen dezentralen, unterschiedlichen nationalen RTGS-Systeme vorangetrieben werden. Ein Erfolgsfaktor für TARGET2 ist die Berücksichtigung der Bedenken der anderen europäischen Länder vor einem deutschen Übergewicht. Vor dem Hintergrund der Osterweiterung der Europäischen Union ist das Projekt zwingend zu realisieren.[800] Wenngleich aus Effizienzgesichtspunkten ein konsolidiertes RTGS-System in Europa wünschenswert wäre, so ist es aus Sicherheitsgesichtspunkten unter Umständen nicht ganz problemlos, auf ein einheitliches europaweites System zu setzen. Gab es bislang im TARGET-Verbund Schwierigkeiten einzelner Systeme, konnten diese einfach vom System getrennt und erst nach Lösung der Probleme wieder zugeschaltet werden. Die unterschiedliche Architektur der Systeme macht es bislang unwahrscheinlich, dass gleichzeitig alle Systeme dem gleichen Problem anheim fallen.

EURO1 als privatwirtschaftliche „Konkurrenz" zu TARGET, zumindest in Bezug auf das Clearing – das Settlement wird weiter über TARGET durchgeführt – und STEP1 lassen auf der Infrastrukturebene die Individual-Zahlungssysteme näher an die Massenzahlungssysteme rücken. Grundsätzlich stellt sich in Zukunft für die Zentralbanken im Eurosystem die Frage, inwieweit privatwirtschaftliche Clearingsysteme im Zahlungsverkehr, die ohne Einflussnahme der EZB betrieben werden, auf Zentralbankgeld als sicheres Verrechnungsmittel rekurrieren können,[801] oder ob diese Möglichkeit aus Effizienz- und Sicherheitsgründen lediglich Systemen rund um TARGET2 offen stehen sollte.

---

[798] Artopoeus (1998), S. 5.
[799] SWIFT (2003a), S. 13.
[800] Vgl. Friederich (2001), S. 13 ff.
[801] So genanntes „prefunding", vgl. Fabritius (2003a), S. 8.

Der Massenzahlungsverkehr steht spätestens seit der Einführung des Euro im Fokus europäischer Politik. Gab die Richtlinie 97/5/EG der Europäischen Union über grenzüberschreitende Überweisungen 1997 in den vorgeschriebenen Minimumstandards lediglich die Laufzeiten einer Überweisung mit 6 Tagen vor, wurde der politische Druck mit der Verordnung 2560/2001/EG über grenzüberschreitende Zahlungen in Euro deutlich erhöht. Die Vorgabe betraf die Gebührenpolitik der Finanzinstitute und forderte gleiche Kosten für nationale wie innereuropäische Überweisungen bis Mitte 2003 (für Beträge bis 12.500 Euro – ab 1.1.2006 wird diese Summe auf 50.000 Euro angehoben), für innereuropäische Kartenzahlungen im Einzelhandel und für Bargeldabhebungen am Geldautomaten (seit 1.1.2002). Der resultierende Kostendruck – und die bis dahin fehlende Kooperation des Finanzsektors auf europäischer Ebene – hatte erhebliche Konsequenzen für die Zahlungssystemlandschaft. Eine institutionelle Folge dieses Drucks war unter anderem die Gründung des European Payments Council (EPC), und dessen für europäische Verhältnisse schnelle Festlegung der Statuten sowie Aufnahme der operativen Tätigkeit. Ferner wurde mit der Inbetriebnahme von STEP2 ein Meilenstein bei der angestrebten Entwicklung eines pan-europäischen automatisierten Clearinghauses (PEACH) erreicht.[802] Die Elektronisierung des Zahlungsverkehrs und der Kostendruck auf der Produktionsseite der Zahlungssystemanbieter lässt das Straight Through Processing von Zahlungen im Großbetrags- und Massenzahlungsverkehr Fortschritte machen. Die Einigung der Finanzinstitute auf die Verwendung internationaler Kontonummern (IBAN) und Bankleitzahlen (BIC) ist ein erstes sichtbares Zeichen dieser Entwicklung. Im Massenzahlungsverkehr kommt es bereits in einigen Ländern bereits mehrmals täglich zum Settlement erfolgter Zahlungen, beispielsweise bei Kreditkartenzahlungen von VISA und MasterCard in Großbritannien.

Die Innovationen im Großzahlungsverkehr wurden von den Zentralbanken einzelner Länder teils entscheidend mitgestaltet, wie das Beispiel Deutsche Bundesbank als Betreiberin des im TARGET-Verbund äußerst erfolgreichen Zahlungssystems RTGS^{plus} zeigt. Dadurch waren regulatorische Bedürfnisse und Anpassungen an veränderte Bedingungen verhältnismäßig einfach innerhalb der jeweiligen Institution zu adressieren. Auch die Weiterentwicklung TARGET2 wird auf Zentralbankebene koordiniert, regulatorische Bedürfnisse können somit verhältnismäßig einfach berücksichtigt werden.

Im Massenzahlungsverkehr stellt sich die Lage unterschiedlich dar. In diesem Segment sind die Zentralbanken in Europa kaum oder überhaupt nicht vertreten und nehmen vielfach eine reine Beobachterposition ein. Bis Ende der neunziger Jahre spielte die Frage der Regulierung dieses Segments – mit der Ausnahme elektronischen Geldes (eMoney)[803] – für viele Zentralbanken keine Rolle. Die zunehmende Elektronisierung in diesem Segment, verbunden mit der Einführung möglicherweise (system-)kritischer Prozeduren, hat jedoch einen Wandel bewirkt. Für systemrelevante Massenzahlungsysteme, und solche von besonderer Bedeutung für die jeweilige Volkswirtschaft, hat das Eurosystem Mitte 2003 einen Anforderungskatalog erstellt, der sich an den „Core Principles for Systemically Important Payment Systems“ orientiert. Damit ist ein erster Schritt in Richtung konzeptionell einheitlicher Vorgaben im Massenzahlungsverkehr gegangen. Die konkrete Ausgestaltung der „Core Principles“ lässt noch auf sich warten, zunächst werden im Eurosystem die jeweiligen Massenzahlungssysteme kategorisiert.

In jüngster Zeit finden sich vermehrt Äußerungen, die einen weiteren Richtungswandel aufzeigen. Waren bislang die elektronischen Retail-Zahlungssysteme, die sich rund um das Internet und mobile Netze entwickelten, kaum beachtet, betonen die Zentralbanken des

[802] Vgl. Friederich (2001), S. 7, Fabritius (2003a), S. 5f.
[803] Vgl. Hartmann (2000).

Eurosystems vermehrt die mögliche Bedeutung dieser Systeme und die Folgen für die Aufsicht und Überwachung. Beispielsweise folgert Fabritius in seiner Analyse der Rolle der Zentralbanken bei Zahlungssystemen im Hinblick auf ePayments:[804] „Rapid technological change in e-payment instruments and procedures and the fragmented evolving market are sufficient reasons for the central banks to streamline their role as overseers." Die BIZ widmet sich ebenfalls auf internationaler Ebene der Rolle der Zentralbanken und der Aufsicht im Bereich des Massenzahlungsverkehrs. Im März 2003 erschien der Bericht „Policy issues for central banks in retail payments", in dem weltweit die operative Beteiligung von Zentralbanken bei diesen Systemen, die Marktentwicklung und deren Auswirkung auf die Effizienz und Sicherheit der Systeme sowie mögliche Gestaltungsansätze der Regulierer diskutiert werden.[805]

„Just as fiat money replaced specie-backed paper currencies, electronically initiated debits and credits will become the dominant payment modes, creating the potential for private money to compete with government-issued currencies."[806] Es ist im Vergleich zur Euphorie Mitte der neunziger Jahre heute sicherlich einfach festzustellen, dass die optimistischen und für Zentralbanken fast apokalyptisch anmutenden Prognosen der Informationsgesellschaft in Bezug auf künftige Zahlungssysteme noch eine Weile auf sich werden warten lassen. Gleichwohl sind die Produktentwicklungen im Retail-Zahlungsverkehr eindrucksvoll. Mit fortschreitender Technisierung sind in der Kette Händler-Zahlungssystem-Dienstleister/Bank-Kunde vielfältige Zahlungssystemansätze denkbar, oder bereits zu beobachten. Obwohl der entscheidende Durchbruch einzelner Systeminnovationen am Markt weiter aussteht, ist die Erwartungshaltung verschiedener Industrien so hoch, dass weitere Bezahlsysteme konzipiert und auf den Markt gebracht werden. Zwei große Entwicklungsrichtungen lassen sich identifizieren. Erstens wird vermehrt Gebrauch gemacht von mobilen Technologien; die tragbaren Kleincomputer/-telefone werden immer leistungsfähiger, eine schnelle Internetanbindung zu tragbaren Kosten scheint eine Frage der Zeit. Die Versorgung mit WLAN-Hot Spots[807] nimmt nicht nur in Deutschland beständig zu – vor allem seit Abrechnungsmodule für deren Nutzung bestehen. Die Konsumenten scheinen zunehmend bereit, die neuen Technologien einzusetzen; möglicherweise wird für sie der Zusatznutzen sichtbarer. Zweitens wird der Markt der Produktinnovationen und innovativen Dienstleistungen strategisch von einer zunehmenden Zahl an Marktteilnehmern besetzt. Neben den Banken und ihren Tochterunternehmen drängen Telekommunikationsunternehmen mit Bezahllösungen, beispielsweise handypay, auf den Markt. Bankenunabhängige Zahlungssystem-Dienstleister erweitern ihr Portfolio um Bezahlmodule für Endkunden.

In der Übersicht über (Internet-)Bezahlsysteme lässt sich als bedeutendster Trend eine Beschleunigung der Clearing- und Settlementvorgänge beobachten (siehe Abbildung 31). Einerseits rücken der Zeitpunkt des Warenerhalts und der Kontobelastung weiter zusammen, andererseits werden einmal abgerechnete Zahlungen auch schneller in den Netzen der Zahlungssystembetreiber rechtsgültig verrechnet, im Extremfall in Echtzeit. Für die Sicherheit der Systeme hat diese Entwicklung positive Seiten, die unter Umständen die Probleme der zunehmenden Komplexität der Technologie überkompensieren. Die Risiken der Akteure, eine begonnene Transaktion wird nicht mit dem gewünschten Ergebnis zu Ende geführt, sinken erheblich. Der Händler kann beispielsweise bei der entsprechenden vertraglichen Gestaltung der Online-Überweisung sicher sein, sein Geld sicher in dem Moment der getätigten Überweisung zu erhalten. Der Kunde erhält im Gegenzug digitale Ware sofort – agiert der

[804] Fabritius (2003a), S. 4.
[805] Vgl. BIZ (2003b).
[806] Jerry L. Jordan zitiert in Dorn (1997b), S. 1.
[807] WLAN = Wireless Local Area Network.

Händler betrügerisch, wäre eine vertraglich erzwungene Rückabwicklung der Überweisung denkbar. Der Zahlungssystembetreiber geht im Fall der Echtzeit-Abwicklung der Überweisung kein Kreditrisiko für den Händler ein, da Clearing und Settlement zusammenfallen.

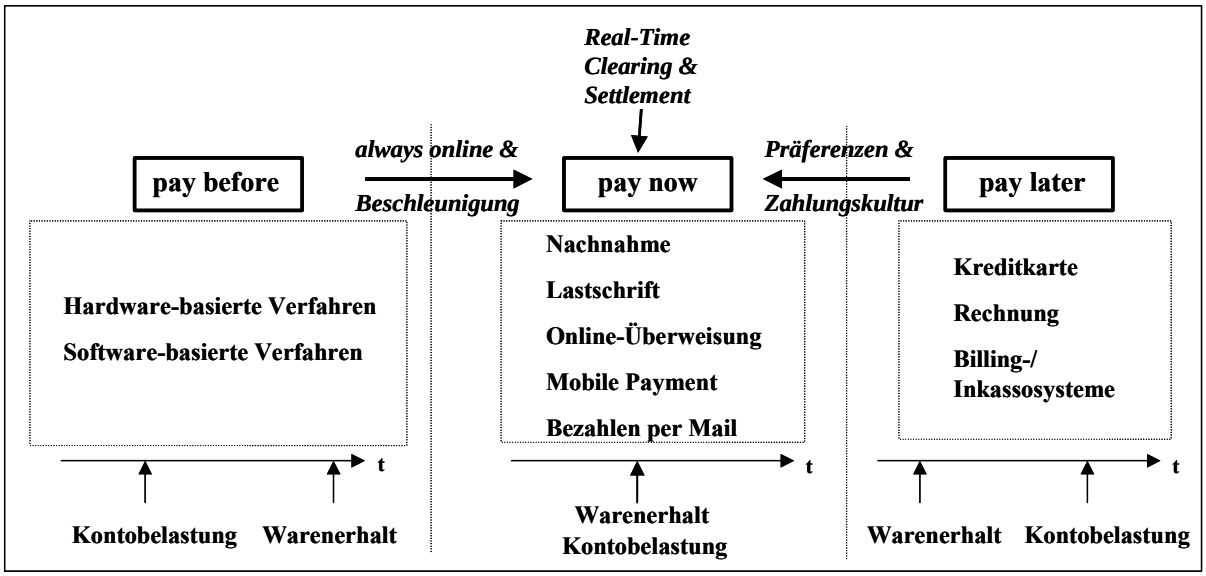

Abbildung 31: Konvergenz der (Internet-)Bezahlverfahren[808]

Noch sind keine „Gewinner" oder eindeutige „Verlierer" dieser Entwicklungen auszumachen. Für die Rolle der Zentralbanken und Aufsicht zeichnet sich jedoch eine zunehmend komplexere Aufgabe ab. Eine größere Anzahl an Unternehmen muss beobachtet und gegebenenfalls reguliert werden. Die legalen Voraussetzungen, innovative Finanzdienstleistungen zur bankerlaubnispflichtigen Bankdienstleistung zu deklarieren, sind gegeben. Allerdings ist eine offene Frage, ob die entsprechenden Behörden personell in der Lage sind, den Markt umfassend zu beobachten und gezielte Einzelprüfungen vorzunehmen. Zudem ist zu klären, inwieweit die Sicherheitskultur der Unternehmen, die nicht der Finanzbranche zugeordnet werden können, das gleiche Niveau erreicht, auf dem sich Aufsicht und Beaufsichtigte bislang eingependelt haben. Die innovativen Anbieter von Zahlungsdienstleistungen haben zwar unter Umständen keine jahrzehntelange Erfahrung in dieser Branche, ihr Vorteil ist es jedoch, dass sie ihre technischen Systeme neu aufsetzen können und keine „Systemdinosaurier" pflegen müssen. Wird bei den neuen Zahlungsverfahren die Sicherheit bereits in der Konzeption konsequent berücksichtigt, kann das Sicherheitsniveau gerade wegen fehlender „Altlasten" sehr hoch sein.

Eine Gegenkraft zur schnellen technologischen Entwicklung stellen die Zahlungsgewohnheiten der Marktteilnehmer dar. Das U.S.-Zentralbanksystem beispielsweise geht von Einsparungen in Höhe von 30 Mrd. bis 50 Mrd. US-Dollar aus, sollte es gelingen, die bis dato größtenteils papiergebundene Scheckverarbeitung auf elektronische Verfahren umzustellen.[809] Trotz der hohen ökonomischen Anreize ist das Beharrungsvermögen des U.S.-amerikanischen Zahlungssystems sehr hoch, und ein schneller Durchbruch innovativer Ansätze ist nicht in Sicht. Selbst bei einer schnellen Entwicklung sicherer Systeme für das Bezahlen im Internet ist nicht gewährleistet, dass Konsumenten und Händler diese in kurzer Zeit annehmen – und dieser Erfolg dazu führt, ein „sonstiges System" in ein „besonderes oder systemrelevantes

[808] Hartmann (2003), geringfügig verändert/ergänzt.
[809] Committee on Banking and Financial Services (2000), S.1.

Massenzahlungssystem“ im Sinne der EZB-Klassifikation zu überführen.[810] Bei entsprechender Gestaltung der Aufsichtsstrukturen bleibt den Regulatoren im Einzelfall hinreichend Zeit, angemessen auf die jeweilige Entwicklung zu reagieren.

Auf Seiten traditioneller Zahlungssystemanbieter, den Finanzinstituten, lässt sich in den letzten Jahren beobachten, dass Rationalisierungspotenziale über kooperative Ansätze realisiert werden sollen. Neben dem Outsourcing nahezu vollständiger IT-Abteilungen an große Systemanbieter wie IBM wird versucht, über die Gründung so genannter Transaktionsbanken den Teil der Prozesse, der zur Markenbindung keinen Beitrag leistet, aber hohe Skaleneffekte aufweist, gemeinsam zu verarbeiten. Im deutschen Zahlungsverkehr spielt in dieser Hinsicht beispielsweise die Postbank AG eine Rolle, die sich vorbereitet, die Abwicklung des Zahlungsverkehrs der Deutschen Bank AG zu übernehmen. Diese Entwicklung ist nicht nur für inländische Häuser denkbar, es ist ebenso vorstellbar, dass europäische Zahlungssystemanbieter die Verarbeitung ihrer Zahlungstransaktionen an gemeinsame Clearinghäuser weiterreichen, um für den europäischen Wettbewerb in der SEPA gerüstet zu sein. Unter dem Aspekt der Sicherheit stellen solche Konstrukte auch an die Aufsicht neue Anforderungen, die EZB hätte personell auf vermehrt europäisch agierende Anbieter zu reagieren, da im Zweifelsfall deren Aktivität nicht mehr klar nationalen Aufsichtsorganen zugeordnet werden kann.[811] Wird die Spezialisierung dieser Clearinghäuser weiter vorangetrieben, und sind die darunterliegenden Prozesse sicherheitstechnisch klar spezifiziert, könnte die Sicherheit des Zahlungsverkehrs weiter erhöht werden – sofern nicht die Schnittstellen/Abstimmungsproblematik Synergievorteile zunichte macht. Die Pläne, im Massenzahlungsverkehr nicht „nur“ europäische sondern weltweite Zahlungstransaktionen zu bearbeiten, die beispielsweise im U.S.-amerikanischen Projekt WATCH ihren Niederschlag finden, sind in der Konsolidierungsphase der Finanzwelt im Eurosystem Zukunftsmusik.[812] Gleichwohl implizieren solche Ambitionen im Hinblick auf Aufsichtsstrukturen anspruchsvolle Fragestellungen.

Für die aufsichtliche Überwachung stellen Organisationen, die aufgrund bereits realisierter Skaleneffekte international operieren, und die für die systemische Sicherheit kritisch sind, beispielsweise SWIFT, eine besondere Herausforderung dar. Für die Aufsicht von SWIFT wurde eine spezielle Vereinbarung auf Zentralbankebene getroffen, die die aufsichtliche Überprüfung von SWIFT regelt. Dabei agiert die belgische Zentralbank am Hauptsitz von SWIFT als federführendes Aufsichtsorgan und koordiniert neben der täglichen Aufsichtsarbeit die aufsichtlichen Vorgaben, die aus den G-10 Ländern über das CPSS der BIZ an die Organisation herangetragen werden. Als Hauptziel der Aufsicht werden die Strukturen und Prozesse von SWIFT in Hinblick auf ein funktionierendes Risikomanagement untersucht. Grundsätzlich finden Prüfprozeduren wie Audits nicht durch Zentralbankpersonal statt, es werden externe Prüfberichte für die aufsichtliche Einschätzung der Lage herangezogen. So ist SWIFT beispielsweise für 2002 nach ISO 17799 zertifiziert. Gleichwohl kommt die Aufsicht am Ende umfassender Prüfungen zu der Aussage:[813] „the G-10 central banks are not precluded from organising the oversight of SWIFT in a different way in the future. This oversight does not grant SWIFT any certification, approval or authorisation; SWIFT continues to bear the responsibility for the security and reliability of its systems, product and services.” Letztere Aussage weist die Verantwortung für Schäden an das geprüfte Unterneh-

[810] Vgl. Leibold (2003).
[811] Eine analoge Problematik zeigt Berentsen (1997) im Zusammenhang mit supranational agierenden Internetbanken und deren Regulierung/Aufsicht auf.
[812] Vgl. zur Diskussion um WATCH, PEACH und Garagen-Clearing aus Zentralbankensicht Friederich (2001), S. 7 ff.
[813] SWIFT (2003a), S. 42.

men zurück. Kein Problem bei geringfügigen Schäden; würde jedoch wirklich ein systemischer Schadensfall in die Milliarden Euro gehen können, wäre allein mit der theoretischen Schuldzuweisung nichts gewonnen. Weder Rücklagen noch Versicherungen wären in diesem Fall in der Lage, den Status Quo wieder herzustellen. Kooperative Mechanismen der Risikoprävention erscheinen bei dieser Sachlage als Königsweg, da Informationsasymmetrien abgebaut werden können.

Die Konzentration von Zahlungsdienstleistern und -dienstleistungen birgt neben Rationalisierungsgewinnen aus Sicherheitssicht grundsätzlich die Gefahr kritischer Flaschenhälse. Diese sind mit dem 11. September 2001 und der daraus folgenden Neubewertung kritischer Infrastrukturen vermehrt in den Blickpunkt des Interesses der Regulierer geraten. Während auf U.S.-Seite mit den hohen Infrastruktur-Standards, die im „Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" vorgegeben werden, diesen Risiken begegnet werden soll, hält sich das Eurosystem mit solchen Vorlagen bislang zurück.

6.2 Problemfelder der Regulierung

„I have been sitting on the Basel Committee for four years, and I still do not understand how decisions are made."[814]

Sicherlich ist die Äußerung von Jerry Hawke zur Entstehung von Regulierung pointiert, ein Körnchen Wahrheit mag sie gleichwohl beinhalten. Zwei Problemfelder der Regulierung lassen sich identifizieren. Zum einen der Bereich der Überregulierung, ein politisches Dauerthema, zum anderen die Problematik sich verändernder Kriterien für die aufsichtliche Beurteilung regulativer Vorgaben. Im Bankenumfeld lässt sich vermehrt der Übergang von quantitativen zu qualitativen Elementen der regulatorischen Gestaltung feststellen. Dies bringt – nicht nur im Zahlungsverkehr – besondere Schwierigkeiten mit sich, die die Aufgaben der Aufsicht in einem neuen Licht erscheinen lassen.

6.2.1 Themenbereich Überregulierung

Die Kritik an der Regulierung dürfte bis in ihre Anfänge zurückreichen. Auch wenn im Wesentlichen unstrittig ist, dass nur durch Regulierung und Aufsicht ein effizienter, wettbewerbsfähiger und stabiler Finanzsektor garantiert werden kann, erreicht in Zeiten des Umbruchs bestehender Strukturen die Kritik an bestehenden Regelungen, die zusätzlich unter Umständen noch weiter verschärft werden sollen, meist den Höhepunkt. Zwei wesentliche Umbruchsitutationen für das deutsche Finanzgewerbe lassen sich ausmachen: Basel II und die Harmonisierung europäischer Regulierungen. Letztere reicht bis weit in die neunziger Jahre zurück – bereits bevor Basel II absehbar war, kritisierten die Banken die Regulierer, insbesondere das Bundesaufsichtamt für das Kreditwesen; es war von Überregulierung und „Regulierungswut" die Rede.[815] Die Mindestanforderungen an das Kreditgeschäft werden in Deutschland als Vorstufe zur zweiten Säule der Basel II Regelungen gesehen. Während die Änderung aufsichtlicher Vorgaben in Richtung qualitativer Aspekte von der Bankenwelt positiv aufgenommen wird, werden die weitreichenden MaK-Bestimmungen gerade für kleinere Institute stark kritisiert; es ist auch hier von Überregulierung die Rede.[816] Mit Basel II wird nunmehr ein Regulierungsrahmen vorgegeben, der vielfach in nationales Recht – in Europa in europäisches Recht – umgesetzt werden soll. Diese Arbeiten sind ebenfalls von

[814] Jerry Hawke, US Comptroller of the Currency in Mander (2003), S.2.
[815] Vgl. Büschgen (1999), S. 273.
[816] Vgl. VÖB (2002), S. 2f., Hofmann (2002), S. 39.

vielfältiger, teils irrational anmutender Kritik begleitet worden. Beispielsweise formuliert Terres:[817] „Insgesamt ist der neue Vorschlag zur Überarbeitung der Eigenkapitalübereinkunft jedoch wieder davon geprägt, vor allem die Kompetenzen der aufsichtsrechtlichen Bürokratie gegenüber den Kreditinstituten zu stärken und die Banken mit **neuen bürokratischen Regulierungen** zu überziehen. Die Folge der Übereinkunft wird eher darin liegen, neue Stellen bei der Bankenaufsicht zu schaffen und mit aufsichtsrechtlichen Mitteln eine – euphemistisch gesprochen – „Marktbereinigung" herbeizuführen als die Sicherheit des Finanzsystems zu stärken."

Bereits vor der Gründung einer deutschen Allfinanzaufsicht war auf Seiten des BAKred eine marktorientiertere Lösung der Regulierungsmaßnahmen im Gespräch, aufbauend auf einer höheren Selbstverantwortung der Institute. Ein Vorteil wäre, die jeder Regulierung innewohnende Tendenz zu pauschalen Regelungen zugunsten institutsindividueller Lösungen, die deren spezifische Besonderheiten berücksichtigen, auszuhebeln. Diese Problematik bezieht sich insbesondere auf die in einigen Geschäftsbereichen, z. B. dem Kreditsektor, großen Unterschiede hinsichtlich Geschäftspraktiken und Risiken zwischen genossenschaftlichen Banken und Sparkassen auf der einen Seite und den Geschäftsbanken auf der anderen Seite.[818] Basel II unterstützt diesen Ansatz in einigen Punkten, beispielsweise wird der Supervisory Review Process in Säule 2 zu verstärktem Wissensaustausch zwischen einzelnen Instituten und der Aufsicht führen. Die Offenlegungspflichten in Säule 3 – die jedoch bereits während der Konsultationen erheblich reduziert wurden – tragen ihr Übriges dazu bei.

Die Überregulierung eines Sektors kann auch daran festgemacht werden, dass die Regulierer selbst beginnen, den Überblick über ihre eigenen Regularien zu verlieren – ganz abzusehen von der noch komplexeren Abstimmungsproblematik vertikaler Regulierung, die von EU-Ebene bis auf Institutsebene konstistent sein sollte. Die Schwierigkeiten der Abstimmung von immer neuen Vorschriften, Empfehlungen und Verordnungen wird in Deutschland bereits innerhalb einzelner Aufsichtsorgane deutlich. Beispielsweise schreibt der Präsident des BAKred am 12.09.2001[819]: „Durch die Veröffentlichung des Rundschreibens 1/2000 über Mindestanforderungen an die Ausgestaltung der Internen Revision der Kreditinstitute [...] kommt es bei einzelnen Regelungen im Hinblick auf die Interne Revision zu Überschneidungen mit meiner Verlautbarung vom 23. Oktober 1995 über Mindestanforderungen an das Betreiben von Handelsgeschäften." Sofern diese Überschneidungen innerhalb der Vorgaben einer Aufsichtsbehörde vorkommen, sind Lösungen aufgrund der eindeutigen Kompetenzlage unproblematisch zu finden. Schwieriger wird es bei unterschiedlichen Institutionen und eventuell gegenläufigen Interessenlagen. Neben der politischen Machtfrage, welche Institution die Regelungen einer anderen dominiert, kann es bei vorhandenem europäischen Abstimmungsbedarf schwierig werden, einheitliche und konsistente Lösungen zu erarbeiten. Auf europäischer Ebene beklagt die Europäische Kommission selbst die babylonische Vielfalt von Vorschriften im Zahlungsverkehr:[820] „Das Nebeneinander dieser zentralen Rechtsakte (2650/2001/EG, 97/5/EG und 97/489/EG Anmerkung d. V.) ist verwirrend, da sich mehrere Bestimmungen überschneiden. Einige Vorschriften der Richtlinie sind nach Erlass der Verordnung hinfällig geworden."

Die Frage der Überregulierung der Finanzmärkte geht einher mit der Frage nach den Instrumenten, die von den Regulierern eingesetzt werden (dürfen). Im Zahlungsverkehr werden insbesondere die Initiativen der Europäischen Union zum grenzüberschreitenden

[817] Terres (2001), S. 1, Hervorhebungen durch den Verfasser.
[818] Vgl. Büschgen (1999), S. 273f.
[819] BAKred (2001), Tz. 1.
[820] KOM (2003b), S. 10.

Zahlungsverkehr kontrovers diskutiert. Die betroffenen Banken, die sich mittlerweile nolens volens konstruktiv auf die neue Situation eingestellt haben, waren zu Beginn teils sehr ungehalten über das Vorgehen der EU-Administration. Rehm beispielsweise kritisierte den aus der EU-Verordnung 2560/2001/EG resultierenden Eingriff in die Preisautonomie der Institute aufs schärfste, und bezweifelte die Legitimation der Regulierer, in dieses Marktsegment einzugreifen:[821] „Dieses ist so nicht akzeptabel. Es ist aus keinem Vertrag oder keiner Verordnung herzuleiten, dass der Europäische Gesetzgeber ermächtigt oder verpflichtet ist, eine Preisangleichung im Binnenmarkt herzustellen."

Eng verbunden mit der Diskussion um eine Überregulierung des Finanzsektors ist die Frage nach der Wirksamkeit des jeweiligen regulatorischen Regimes. Darüber gehen die Meinungen auseinander. Die eine Seite ist mit den bestehenden Regularien und Institutionen durchaus zufrieden und kann sich eine zunehmende Hierarchisierung zumindest auf europäischer Ebene – beispielsweise eine europäische Allfinanzaufsicht[822] – vorstellen. Zeitler beispielsweise argumentiert für das weitgehende Beibehalten des Status quo und begründet dies mit den Erfolgen der Vergangenheit. Die Aufsichtsstrukturen hätten die Stabilität des Finanzsektors weitestgehend auch in Krisen garantiert, und zusätzlich wären Lehren aus den jeweiligen Erfahrungen gezogen worden. Gleichwohl wünscht er sich bei der Bankenaufsicht eine wirksame Kooperation, um den neuen Herausforderungen gewachsen zu sein, einen schnelleren Informationsaustausch und enge Abstimmungen sowie standardisierte Aufsichtsprinzipien.[823] Zumindest der Informationsaustausch zwischen Aufsichtsorganen und internen sowie externen Auditoren wird teilweise bereits gepflegt. Beispielsweise werden die Auswirkungen neuer Regulierungen auf die Arbeit der Auditoren und der Aufsicht im Zusammenhang mit einer Neuordnung der Internen Revision bei Banken konstruktiv diskutiert. Die Zusammenarbeit von Revisoren und Aufsicht muss gesetzlich verankert sein, sonst entstehen neue Risiken beispielsweise in Form von Haftungsfragen, wenn eine bankinterne kritische Information nach Außen dringt.[824] Diese Thematik spielt bei der Implementierung des Supervisory Review Process nach Basel II eine wesentliche Rolle, da hier Revision und Aufsicht weitaus mehr zusammenarbeiten werden als bisher. Der aufgrund der Verflechtungen in der deutschen Finanz- und Versicherungswirtschaft ebenfalls notwendig gewordenen Zusammenarbeit der einzelnen Aufsichtsorgane in Deutschland wurde organisatorisch mit der Gründung einer Allfinanzbehörde – der BAFin – begegnet. Auf europäischer Ebene steht eine ähnliche Diskussion noch aus.[825]

Die andere Seite sieht gerade auf EU-Ebene starke Probleme bei der Umsetzung eines einheitlich regulierten Finanzmarktes. So stellt der Ausschuss der Weisen in seinem Abschlussdokument zur Analyse des Marktes für Finanzdienstleistungen am Beispiel der Regulierung der europäischen Wertpapiermärkte erhebliche Defizite bei den bisherigen Regulierungsmechanismen fest.[826] Auf den Punkt gebracht, formuliert der Rat ungewöhnlich scharf:[827] „Das Problem ist nur zum Teil die unvollständige Regelung auf europäischer Ebene. Hauptursache ist vielmehr die Art und Weise, wie EU-Recht gesetzt (oder eben nicht gesetzt) und "umgesetzt" (bzw. nicht "umgesetzt") wird. Kurz: Das Problem ist das System selbst." Baldwin und Cave kommen in ihrer Analyse der Regulierung im europäischen Kontext zum Schluss, dass eine einheitliche Anwendung europäischen Rechts nur dann funktionieren

[821] Rehm (2001), S. 7.
[822] Schmidt (2001) zur Diskussion um die Allfinanzaufsicht, S. 6 ff.
[823] Vgl. Zeitler (2000), S. 11 ff.
[824] Vgl. BIZ (2002f), S. 8 ff. Der Streitfall Leo Kirch versus Deutsche Bank zeigt die Brisanz dieser Problematik.
[825] Vgl. Schmidt (2001).
[826] Vgl. Ausschuss der Weisen (2001), S. 19ff.
[827] Ausschuss der Weisen (2001), S. 19.

könnte, wenn innerhalb des Systems hinreichend für Transparenz gesorgt würde – ein schwieriges Unterfangen.[828] Gleichwohl wird in ersten ambitionierten Ansätzen versucht, in ausgewählten Problembereichen wie der Wertpapierabwicklung, das so genannte Lamfalussy-Modell zur Konsolidierung europäischer Regulierungsmaßnahmen umzusetzen. In einem 4-Stufen-Prozess sollen dabei Rahmengesetze verabschiedet (Stufe 1), Umsetzungsmaßnahmen beschlossen (Stufe 2), gemeinsame Empfehlungen, Auslegungen von Standards etc. erarbeitet (Stufe 3) und schließlich deren Einhaltung von der EU-Kommission überwacht werden (Stufe 4).[829] Auch wenn die bisherigen Erfahrungen für den Wertpapiersektor insbesondere in den Stufen 3 und 4 noch als schwierig eingestuft werden können, so ist bereits von einer Ausweitung des Lamfalussy-Verfahrens auf den gesamten Finanzsektor der EU die Rede.[830]

Wird der einheitliche europäische Finanzbinnenmarkt in einer erweiterten Union Realität, sind institutionelle Reaktionen unvermeidlich. Die Vorschläge reichen von einer kohärenten Zusammenarbeit der nationalen Regulierungs- und Aufsichtsbehörden bis hin zur Forderung nach einer einheitlichen Aufsichtsstruktur auf europäischer Ebene, die in letzter Instanz mit einer EU-Regulierungs- und Aufsichtsbehörde (EFSA (European Financial Services Agency)) einhergeht.[831]

6.2.2 Kriterien aufsichtlicher Überprüfung im Spannungsfeld quantitativer Normen und qualitativer Ansätze

Es lässt sich eine Tendenz zu qualitativen Normen im Bereich Risikomanagement feststellen. Für die Markt- und Kreditrisiken scheinen die rein quantitativen, externen Vorgaben an ihre Grenzen gestoßen. In den letzten Jahren wurden zunehmend bankinterne Ansätze entwickelt, die Einfluß auf die regulatorische Gestaltung genommen haben. Der Aufsicht obliegt es nunmehr, die qualitativen Anforderungen an diese Ansätze und an die Umgebung, in der sie operieren, auszuformulieren. Für die Kreditrisiken im Besonderen und das Risikomanagement im Speziellen kommt Artopoeus allerdings bereits 1998 zu einer ebenso nüchternen wie pragmatischen Erkenntnis:[832] „Für die Aufsichtsbehörden ist eine solche qualitative Aufsicht freilich eine schwierige Gratwanderung. Risikomanagement ist die ureigene Verantwortung der Banken selbst. Bankaufsichtsbehörden können und dürfen nicht in die Geschäftspolitik und Organisation einer Bank eingreifen und insbesondere nicht versuchen, ihre eigenen Vorstellungen von der Art und Weise, wie eine Bank ihre Geschäfte betreiben sollte, durchzusetzen. Bankaufseher sind nicht die besseren Banker."

Die bisherige Praxis quantitativer Prüfnormen gibt der Aufsichtsbehörde die Möglichkeit, bei Mangel an eigenem Prüfpersonal unabhängige Dritte zu beauftragen. In Deutschland erfüllen neben den Prüfern der Deutschen Bundesbank und der BAFin externe Wirtschaftsprüfer die Aufgabe der Überprüfung aufsichtlicher Normen. Aus Effizienzgesichtspunkten wäre eine Integration aufsichtlicher Ziele in die Unternehmensziele ideal. Ausgangspunkt einer solchen Überlegung ist die Annahme, dass das Bankmanagement über detaillierte Informationen verfügt, und die interne Steuerung intrinsisch motiviert besser funktioniert als von außen auferlegte Vorgaben.[833] Eine solche Konformität bei der Zielerfüllung könnte beispielsweise über eine hinreichende Anreizsystematik für die Geschäftsbanken erreicht werden, und die problematische Informationsasymmetrie zwischen Aufsicht und Beaufsichtigten neutralisieren. Einen ersten Ansatz für anreizkompatible aufsichtliche Maßnahmen dieser Art bietet

[828] Baldwin (1999), S. 179.
[829] Vgl. Ausschuss der Weisen (2001), S. 10.
[830] Vgl. Kern (2003), S. 11.
[831] Vgl. Ausschuss der Weisen (2001), S. 21 und 28, Kern (2003), S. 11.
[832] Artopoeus (1998), S. 4.
[833] Vgl. Diskussion bei Burghof (1996), S. 112 ff.

Basel II. Dort wird der Versuch unternommen, den Einsatz ausgefeilter Risikomess- und Steuerungsmodelle bei den Geschäftsbanken über eine reduzierte Anforderung an die Eigenkapitalausstattung zu motivieren. Ob jedoch die Höhe des in Basel II angedachten Anreizes ausreichend ist, scheint fragwürdig.[834]

Burghof und Rudolph haben jedoch keine zu großen Erwartungen im Hinblick auf eine Konvergenz von Aufsichts- und Unternehmensinteressen; aus ihrer Sicht ist ein Hauptziel der Aufsicht das Vermeiden von Konkursen, für die Geschäftsbanken ist dies lediglich eine Nebenbedingung, die Profitmaximierung das Hauptanliegen. Die Schwierigkeiten bei der Durchsetzung quantitativer Normen lässt die Autoren von einer „Krise der quantitativen Normen" sprechen, die zu einem Trend in Richtung qualitativer Elemente geführt hat.[835]

Methodisch ist insbesondere die technische Sicherheit von (IT-)Systemen schwierig zu quantifizieren. Zwar lassen sich mit Hilfe von Prüfnormen wie den Common Criteria[836] verschiedene Sicherheitslevels (EAL 1 (niedrige Schutzstufe) bis EAL 7 (höchste Schutzstufe, Sicherheit mit formalen Modellen überprüft)) definieren, die allerdings nur begrenzt anwendbar erscheinen. Zum einen ist es fast unmöglich, bestehende Systeme retrospektiv nach hohen Prüfnormen, EAL 4 und höher, zu prüfen, ohne diese Systeme komplett neu aufzubauen. Zum anderen ist damit der erweiterte Sicherheitsbegriff noch nicht abgedeckt, und bisher ist es nur in Ansätzen gelungen, formale Methoden auch bei komplexen Systemen unter Einbezug technisch-organisatorischer Fragestellungen durchgängig anzuwenden. Dies wäre allerdings eine zwingende Voraussetzung für die wirksame Quantifizierung von Normen. Kosten-Nutzen-Relationen sind an dieser Stelle nicht berücksichtigt und würden vermutlich die alleinige Anwendung formaler Methoden bei komplexen Systemen zusätzlich erschweren. In einzelnen Feldern, die zudem, da sie kaum eine Historie haben, überschaubar erscheinen, wagen sich Regulierer jedoch an klare formale Sicherheitsvorgaben. Das jüngste Beispiel sind die „Electronic Money System Security Objectives" der EZB, die weiter gemäß den Richtlinien der Common Criteria ausgebaut werden sollen.

Die erwähnten Schwierigkeit vor Augen gehen die Regulierer vermehrt einen anderen Weg, den Artopoteus bereits 1998 vorgezeichnet hat: Die Aufsicht müsse letzlich aus Mangel an Alternativen bei bestimmten Situationen mit qualitativen Anforderungen im Sinne von „best practices" operieren.[837] Er fordert allerdings die beaufsichtigten Kreditinstitute zur eigenständigen Entwicklung solcher Leitlinien in Kooperation mit der Aufsicht auf und spricht sich für Ansätze der Selbstregulierung aus. Ein anschauliches Beispiel für eine qualitative Vorgabe dieser Art bieten die in Kapitel 5.3 diskutierten „Sound Practices for the Management and Supervision of Operational Risk", die im Zuge der Basel II Konsultationen entstanden sind. In die gleiche Richtung gehen die Vorgaben für Großzahlungssysteme mit den „Core Principles for Systemically Important Payment Systems" und im Bereich eBanking die „Risk Management Principles for Electronic Banking".

Ein Problem quantitativer Normen und Vorgaben bei Prüfungen kann die Aufsicht mit qualitativen Normen umgehen: Ein von Schäden betroffenes Kreditinstitut kann nicht argumentieren, es hätte bestimmte Anforderungen auf den Punkt erfüllt, und würde nun die Aufsicht für die Folgeschäden, die trotzdem oder gerade deswegen eingetreten seien, haftbar machen wollen. Die Auslegung qualitativer Vorgaben ist dehnbar, sowohl von den Instituten als auch von der Aufsicht – ein Argument mehr für einen kooperativen Ansatz in bestimmten

[834] Für Operationelle Risiken wird dies in BIZ (2001c), S. 1 f. näher ausgeführt.
[835] Burghof (1996), S. 112.
[836] Vgl. ISO 15408-1(1999).
[837] Vgl. Artopoeus (1998), S. 3 ff.

Bereichen, in denen sich qualitative Vorgaben als Königsweg zu erweisen scheinen. Allerdings sind ohne Rechtswirksamkeit weder qualitative noch quantitative Normen durchsetzbar.

Qualitative Normen bringen für die Aufsicht jedoch neue Probleme mit sich. Wer überprüft deren Einhaltung? Können bei quantitativen Normen trotz aller Probleme einer korrekten Ermittlung und Berechnung vorgegebener Prüfzahlen, Wirtschaftsprüfer zur Überprüfung dieser Vorgaben eingesetzt werden, mit der Folge einer entsprechenden personellen Entlastung der Aufsicht, ist diese Möglichkeit bei qualitativen Vorgaben zumindest bedenklich. Qualitative Normen lassen Interpretationsspielraum, der im Ernstfall, in Ermangelung quantitativer Ableitungen, zu juristischen Streitigkeiten zwischen Geschäftsbanken und Aufsicht führen könnte.[838] Diese Problematik wird im Fall technischer Zielvorstellungen verschärft. Der Interpretationsspielraum regulativer Vorgaben könnte lediglich dadurch eingeschränkt werden, dass die Aufsicht selbst mit eigenen Mitarbeitern anhand eines für alle Akteure nachvollziehbaren Schemas prüft, oder die Offenlegungspflichten so hoch werden, dass die interessierte (Fach-)Öffentlichkeit Risiken selbst einschätzen kann.

Die Vorteile eines in Abschnitt 5.3.3 entwickelten Risikomanagementansatzes für Operationelle Risiken sind offensichtlich: Es kann bis zu einem bestimmten Grad – weiter als bisher – die Dichotomie von quantitativen und qualitativen Vorgaben aufgelöst werden. Die Aufsicht ist in den Risikomanagementprozess involviert, kann die aufgetretenen Schadensfälle in gleicher Position wie die Kreditinstitute analysieren und eigene über die Maßnahmen der Institute hinausgehende Regulierungsinstrumente einsetzen. Die Integration der Aufsicht in diesen Prozess vermittelt den Aufsichtorganen in Kombination mit der Entwicklung quantitativer Kennzahlen, beispielsweise der Anzahl Schadensfälle bei Operationellen Risiken, ein, wenngleich zunächst subjektives, Gefühl für das relevante Marktgeschehen. Zudem wird für die Kreditinstitute ein Argument entkräftet, das in Verbindung mit Regulierung häufig genannt wird – es würden mit jeder neuen Regulierungsmaßnahme neue Kosten auf die Institute zukommen. Ein gut etablierter Risikomanagementprozess wie oben dargelegt, hätte nach Meinung des Autors beste Chancen, die Kosten-Nutzen-Relation zugunsten der beaufsichtigten Kreditinstitute zu verschieben.

Dabei sei zugegeben, dass man sich bei einem Paradigmenwechsel von quantitativen zu qualitativen Vorgaben, aber auch bei Modellen wie dem oben vorgeschlagenen, vermutlich von der Möglichkeit, für Alles und Jedes Testate, Zertifikate und Gütesiegel zu vergeben, verabschieden muss; zumindest teilweise. Ein Ansatz, der den Prozesscharakter des Risikomanagements unterstützt und betont, hat keinen klar definierten Endpunkt, an dem eine Qualitätsendkontrolle stattfinden könnte. Bedingt durch die Dynamik im Markt, in den Technologien und bei den Verfahren lassen sich sehr schwierig, wenn überhaupt, Vergleichswerte zur Beurteilung im Sinne eines festgefügten und weitgehend statischen Benchmarking finden. Die offensichtliche Hinwendung zu qualitativen Vorgaben im Sinne von „core principles“ oder „best practices“ ist im Kern durch die große technologische Dynamik im Bankenumfeld erklärbar. In der Folge werden zunächst Grundprinzipien aufgestellt, die anschließend konkretisierend in den Anwendungszusammenhang gestellt werden müssen, wie beispielsweise bei den CPSIPS geschehen, und auch bei den Mindeststandards für Massenzahlungssysteme der EZB absehbar. Probleme der Dokumentation von sicherheitsrelevanten Details und organisatorischen Bedingungen im dynamischen Betriebs- und Marktumfeld lassen sich dennoch mit qualitativen Vorgaben nicht lösen, sie werden nur gleichsam in die „zweite Reihe“ geschoben und dort unter Umständen weniger wahrgenommen.

[838] Burghof (1996), S. 114. Zu möglichen Zielkonflikten bei allzu vagen qualitativen Vorgaben vgl. das sehr anschauliche Beispiel des § 54 VAG Vermögensanlage (1) bei Burghof (1996), S. 113.

Dessen ungeachtet wird mit Hilfe der nunmehr tatsächlich im Rahmen der Basel II-Vorschläge erfassten Schadensfälle in Folge Operationeller Risiken sowohl in Höhe als auch Häufigkeit eine Qualitätsrichtschnur gezogen. Zumindest unter der Annahme, dass das Meldeverhalten nach entsprechenden Schulungsmaßnahmen der Mitarbeiter ein hohes Maß an Konsistenz aufweist. Die Kritik an den in Basel II skizzierten Verfahren zur quantitativen Messung Operationeller Risiken, verbunden mit der Forderung nach mehr qualitativen Elementen,[839] kann im Zeitverlauf zumindest abgemildert werden. Ist eine genügend große, valide Datenbasis vorhanden – über deren Zustandekommen Aufsicht und Banken die gleichen Informationen haben – können entsprechende Validierungsverfahren wie Backtesting anlaufen. Sollte die Quantifizierung Operationeller Risiken wie oben skizziert gelingen, wird die Aufsicht ein die qualitative Komponente unterstützendes Instrumentarium in Händen halten, das ebenso den beaufsichtigten Instituten zugute kommt. In der Summe der Verfahren kann damit die von Bräuhäuser et al. vorgeschlagene Vorgehensweise eines verstärkt qualitativen Ansatzes für das Management Operationeller Risiken deutlich verbessert werden.[840] Dies gelingt jedoch vermutlich nur in den Branchen, beispielsweise dem Finanzsektor, in denen die Regulierer „top down" Kategorisierungsklassen und Merkmalsausprägungen für Operationelle Risiken definieren, anhand derer die statistisch notwendige Grundgesamtheit an Daten zuverlässig generiert werden kann.

Die Schwierigkeiten der Aufsicht, quantitative bankinterne Ansätze zu validieren, und mit qualitativen Vorgaben an diese zu verknüpfen, ist bereits von der Einführung der Kreditrisikomodelle bekannt. In diesem Zusammenhang kam Artopoeus zu einer Schlussfolgerung, die ebenso für die Modelle Operationeller Risiken gilt:[841] „Die Anerkennung von Kreditrisikomodellen für die Zwecke der Eigenkapitalberechnung wäre ein Quantensprung in der Aufsicht und würde diese vor Herausforderungen ganz neuer Art stellen. Denn bankeigene Kreditrisikomodelle könnten nur dann zugleich auch bankaufsichtlichen Zwecken dienen, wenn sich die Bankaufsichtsbehörden im Einzelfall von ihrer Geeignetheit und Genauigkeit überzeugt haben. Kreditrisikomodelle müssten daher bestimmten bankaufsichtlichen Mindestanforderungen genügen und von den Aufsichtsbehörden jeweils geprüft und zugelassen werden. Damit würde die Qualität bankinterner Mess- und Steuerungsverfahren zum zentralen Gegenstand der bankaufsichtlichen Überwachung; d.h. die Aufsicht würde endgültig zur Qualitätsaufsicht. Für die Arbeitsweise und die Personalausstattung der Aufsichtsinstanzen, aber auch für deren Verhältnis zu den Banken, hätte dies – jedenfalls in Deutschland – weitreichende Folgen." Diese Beurteilung gilt im gleichen Maße, und in Bezug auf die statistische Methodik verstärkt, für die Quantifizierung Operationeller Risiken. Die Aufsicht gerät mit der Evaluation bankinterner Verfahren in die Rolle eines „TÜV" für die Qualität der Mess- und Steuerungsverfahren in Kreditinstituten. Zu dieser Erkenntnis gelangt auch die Deutsche Bundesbank in der aktuellen Diskussion der Folgen der „neuen Aufsicht" nach MaK und Basel II: Die Kreditinstitute einerseits können sich nicht mehr auf regulatorisch gesetzte Definitionen und Abgrenzungen zurückziehen. Sie müssen ihre bankinternen Prozesse optimieren und der Aufsicht kommunizieren. Die Bundesbank/Aufsicht andererseits ist gefordert, Mindestanforderungen an ebendiese Prozesse und Methoden zu formulieren, deren Umsetzung zu überprüfen und zu bewerten.[842]

Der in Basel II formulierte „Supervisory Review Process" berücksichtigt die Tendenz zur Vorgabe qualitativer Normen durch die Aufsicht. Die Idee, Aufsichtspersonal vor Ort zu

[839] Vgl. Jörg (2002), S. 92.
[840] Vgl. Bräuhäuser (2002).
[841] Artopoeus (1998), S. 5 f.
[842] Vgl. Pluto (2003), S. 9.

platzieren, und die laufende Überwachung gleichsam zu institutionalisieren, ermöglicht der Aufsicht, direkt am bankinternen Geschehen teilzuhaben, und nicht nur auf punktuelle Prüfberichte und deren Auswertung angewiesen zu sein. Insbesondere entwickeln die Prüfer vor Ort ein Gefühl für die Risikokultur der Unternehmung und erhalten einen Eindruck von der Fähigkeit der beaufsichtigten Institution, Vorgaben und Normen einzuhalten.

Läuft der SRP effektiv, kommt es nicht erst gegen Ende einer Berichtsperiode zur Feststellung von Fehlverhalten und der daran anschließenden Suche nach geeigneten Sanktionierungsmaßnahmen. Vielmehr wird es möglich, in einem iterativen Prozess Fehlentwicklungen möglichst frühzeitig zu erkennen und gegebenenfalls entgegenzuwirken. Beispielsweise ist vorgesehen, dass die Eigenkapitalanforderungen an einzelne Institute von der Aufsicht über das in Basel II vorgegebene Maß erhöht werden können, sofern die Aufsicht zusätzliche Risiken erkennt.

Weiterführende Sanktionen bei persistentem Fehlverhalten müssen gleichwohl entwickelt werden. Der Weg, den die französische Zentralbank in Hinblick auf Zahlungssysteme geht, erscheint an dieser Stelle interessant: Fehlentwicklungen, die von der Aufsicht nicht geduldet werden können, und die von einem Zahlungssystemanbieter nicht in einer angemessenen Frist behoben werden können oder wollen, führen zur Veröffentlichung einer Warnung durch die Aufsicht im Amtsblatt.[843]

6.3 Überlegungen zur Gestaltung des institutionellen und regulatorischen Umfelds im elektronischen Zahlungsverkehr anhand eines „Rautenmodells" der Regulierung

„Payments in any form, at any time, reflect the degree of trust market participants place in the institutions governing them."[844]

Die Argumentation dieses Abschnitts folgt Dewatripont und Tirole, die postulieren, im Bereich der Bankenregulierung würden einzelne Aspekte, wie die Transformationsaufgabe der Banken, über Gebühr betont, und die Suche nach den Motiven und Zielen der Regulierung vernachlässigt. Während Dewatripont und Tirole den Zahlungsverkehrssektor in ihrer anschließenden ausführlichen Analyse explizit ausschließen,[845] soll an dieser Stelle der Frage nach eben diesen Zielen und Motiven der Regulierung und Regulierer im (elektronischen) Zahlungsverkehr nachgegangen werden.[846]

In Kapitel 3 wurde zwar die Notwendigkeit der Regulierung des Finanzsektors theoretisch fundiert, es wurden jedoch keine Hinweise auf greifbare Effizienzmaße gefunden. Es ist schwierig, Maßstäbe der Regulierung in quantifizierbarer und somit vergleichbarer Form aufzustellen, die qualitativen Aspekte überwiegen letztlich. Burghof und Rudolph gehen noch einen Schritt weiter und kommen zu dem Schluss: „Vor diesem Hintergrund erscheint es sinnvoll, bankaufsichtliche Normen in ihrer konkreten Ausprägung als gewachsene, auf Erfahrungswerten der Aufsichtsbehörden beruhende Leitsätze zu verstehen."[847] Für überschaubare, historisch gewachsene Zusammenhänge und eine im nationalen Kontext eingebettete Aufsicht mit klar definierten Außenbezügen und Schnittstellen mag dieser Ansatz noch tragen; im Bemühen um einen einheitlichen europäischen Wirtschaftsraum und ein „level playing field" der Regulierung ist eine solche Handlungsmaxime als schwierig zu charakteri-

[843] Vgl. Beau (2002), S. 5f.
[844] Santomero, A. M. in: Sienkiewicz (2002), S. 3.
[845] Die für einen späteren Zeitpunkt versprochene Behandlung des Zahlungsverkehrs ist bislang noch nicht erfolgt.
[846] Vgl. Dewatripont (1994), S. 29 ff.
[847] Burghof (1996), S. 33.

sieren. Verschärft wird die Problematik, wenn die Regulierung neben „klassischen“ bankfachlichen Themen in neuster Zeit mit technologischen Entwicklungen konfrontiert wird, die teilweise dezidierte technische Leitlinien, Empfehlungen aber auch Vorschriften erfordern.[848] In Europa stellt sich die Europäische Zentralbank vermehrt dieser Aufgabe. Die EZB muss dabei allerdings mit den durchaus unterschiedlichen Ausprägungen regulatorischer Gestaltung in den Ländern des Eurosystems zurechtkommen. Dies wird bereits an den Stellungnahmen zum Konsultationspapier der EU-Kommission, in dem ein möglicher Rechtsrahmen für den Zahlungsverkehr im Binnenmarkt vorgeschlagen wird, deutlich. Die nationalen Besonderheiten des Zahlungsverkehrs sowie deren Notwendigkeit werden explizit betont.[849]

Im folgenden werden zunächst die Ziele der verschiedenen Regulierer identifiziert, und das so genannte „Rautenmodell“ der Regulierung des Zahlungsverkehrs in Abschnitt 6.3.1 vorgestellt. Anhand dieses Modells kann anschließend der institutionalisierte Rahmen, in dem Zahlungsverkehr in Deutschland und Europa stattfindet, analysiert werden. Wesentliche Fragestellungen berühren die Regulierungsform, die Gewichtung der Regulierungsziele, ihre Position zueinander und die Rolle der verschiedenen in die Regulierung involvierten Institutionen. Wer stimmt beispielsweise die verschiedenen Ebenen der Regulierung aufeinander ab?

Die Schlussfolgerungen der Analyse finden sich in den abschließenden Überlegungen zur Gestaltung des institutionellen und regulatorischen Umfelds im elektronischen Zahlungsverkehrs.

6.3.1 Rautenmodell der Regulierung des Zahlungsverkehrs

In den vorangegangenen Abschnitten, insbesondere in den Kapiteln 4.4 und 5.1, wurde die Motivation und Zielrichtung der aufgeführten regulierenden Institutionen deutlich. In der abstraktesten Form wird durch allgemein gehaltene Empfehlungen auf OECD-Ebene gehofft, den volkswirtschaftlichen Wohlstand der Nationen zu mehren. Werden der Finanzsektor und die darin befindlichen Regulierer auf staatlicher sowie privatwirtschaftlicher Ebene untersucht, können zentrale regulatorische Imperative im Bereich (elektronischer) Zahlungsverkehr herausgearbeitet werden. Dies wird im folgenden exemplarisch anhand der bedeutendsten staatlichen Regulierer weltweit, im Eurosystem und in Deutschland belegt: Europäische Kommission, Europäische Zentralbank, Deutsche Bundesbank und als wichtigem internationalem „Ideengeber“ die Bank für Internationalem Zahlungsausgleich.

Bank für Internationalen Zahlungsausgleich
Ziele, die Zentralbanken insbesondere bei Massenzahlungssystemen berücksichtigen sollten, unterscheiden sich aus Sicht der BIZ nicht von ihren sonstigen Zielen. Die Ziele sind von der jeweiligen Rolle, die eine Zentralbank einnehmen kann, geprägt. Die Zentralbank kann a) selbst Zahlungssysteme (sowohl Massen- als auch Großzahlungssysteme) betreiben, b) die Überwachungsfunktion des Marktes übernehmen und c) eine Katalysatorfunktion wahrnehmen, um den reibungslosen Ablauf des Zahlungsverkehrs zu garantieren. In den “Policy issues for central banks in retail payments” identifiziert die BIZ vier vorrangige Ziele, die von

[848] Vgl. EZB (1999b), S. 8. Allerdings dort ebenfalls darauf hingewiesen, dass die erste Welle „technischer Revolution“ die Bankenstruktur bereits in den sechziger und siebziger Jahren massiv erfasst hat, und die Institute seitdem mit technologischem Wandel konfrontiert sind. Der wesentliche Unterschied erscheint dem Autor in der Tatsache zu liegen, dass im Zuge des Prozesses der Disintermediation neue Anbieter auf dem Bankensektor erscheinen, die die bisher festgefügte vertikale und horizontale Intergration der Wertschöpfung der Banken aufbrechen, vgl. Schilder (2001), S. 1 f.
[849] Vgl. u. a. KOM (2003b), Deutsche Bundesbank (2002b) und ZKA (2002).

den Zentralbanken flankierend oder federführend bei der Wahrnehmung der jeweiligen Rollen verfolgt werden sollten und werden:[850]

1) Der Rechtsrahmen sollte Marktentwicklung und Innovation fördern. Zentrale Aspekte sind dabei die Gewährleistung effizienter und sicherer Marktstrukturen.
2) Der Wettbewerb sollte gefördert werden, notfalls durch Aufnahme eigener Dienste.
3) Die Infrastrukturentwicklung sicherer Zahlungssysteme sollte von der Zentralbank unterstützt und gefördert werden, unter anderem durch die Vorgabe oder Entwicklung entsprechender Standards und Vereinbarungen
4) Die Zentralbank sollte dem Markt ihre eigenen Dienstleistungen möglichst effizient und marktnah zur Verfügung stellen, insbesondere Settlement-Dienste.

Europäische Union

Auf Seiten der EU-Kommission lassen sich die Zielsetzungen des Lissabonner Gipfels und des Aktionsplans für Finanzdienstleistungen heranziehen, um ein deutliches Bild von den angestrebten Zielen innerhalb der Europäischen Gemeinschaft zu bekommen. Gleichsam als Oberziel wird darin das reibungslose Funktionieren der Wirtschaft genannt. Nur wenn diese gewährleistet ist, kann die „Union bis zum Jahr 2010 zum wettbewerbsfähigsten wissensbasierten Wirtschaftsraum der Welt“[851] gemacht werden. Eine wesentliche Bedingung zum Erreichen dieser Ziele sind moderne Zahlungsverkehrsinfrastrukturen, die durch einen geeigneten Rechtsrahmen verbraucherorientiert (Unternehmen und Händler sind in diesem Verständnis auch Verbraucher) ausgerichtet sind. Effizienz und Sicherheit der Systeme müssen zusätzlich erfüllt sein.[852] Der Kommissionsvorschlag eines neuen Rechtsrahmens für den Zahlungsverkehr im Binnenmarkt nennt als Leitprinzipien: „Effizienz als ständiges Ziel“[853], „Sicherheit als Conditio sine qua non“[854], „Wettbewerb: Marktzugang und gleiche Ausgangsbedingungen“[855] und „Kundenschutz auf hohem Niveau“[856].

Europäische Zentralbank

Die Ziele des Eurosystems bei Zahlungssystemen werden von der EZB im Rahmen der Selbstpositionierung in einem Grundlagenpapier für die Überwachungsfunktion und einem weiteren Übersichtsartikel zur Rolle des Eurosystems bei Zahlungs- und Verrechnungssystemen formuliert.[857] Die EZB positioniert sich bislang lediglich als Betreiberin des Settlement-Systems TARGET innerhalb des Eurosystems, eine Betreiberrolle im Massenzahlungsverkehr scheint nicht angedacht. In diesem Bereich wird vielmehr die Katalysatorfunktion der EZB betont.[858] Dort spielt die Förderung eines fairen Wettbewerbs der verschiedenen Anbieter, insbesondere länderübergreifend, eine zentrale Rolle. Im Hinblick auf die Überwachungsfunktion, die sich aus dem gesetzlichen Auftrag und dem EU-Vertrag ableiten lässt, werden als Ziele, respektive Gründe, für diese Funktion genannt:

- Die systemische Stabilität soll gewährleistet werden.
- Die Effizienz der Systeme ist zu sichern.
- Die Sicherheit der Systeme muss überwacht werden.

[850] Vgl. BIZ (2003b), S. 4 f.
[851] KOM (2003b), S. 8.
[852] Vgl. KOM (2003b), S. 8.
[853] KOM (2003b), S. 12.
[854] KOM (2003b), S. 13.
[855] KOM (2003b), S. 14.
[856] KOM (2003b), S. 15.
[857] Vgl. EZB (2000b) und EZB (2002b).
[858] Vgl. EZB (2002b), S. 61.

- Zahlungssysteme als Transmissionskanal für eine wirksame Geldpolitik müssen funktionieren.

Die Überwachungsfunktion wird gewährleistet, indem die EZB Standards festlegt oder vorgibt, die sicheren, zuverlässigen und effizienten ZV gewährleisten sollen, und deren Einhaltung überwacht. Zusätzlich hat die EZB die Aufgabe, den Markt zu beobachten, um rechtzeitig über eventuell bedeutende Entwicklungen informiert zu sein und reagieren zu können.[859] Dabei soll im elektronischem Zahlungsverkehr zunächst die Katalysatorfunktion betont werden, und erst sobald der Markt auf eigenen Füßen steht die Überwachungsaufgabe.[860] Das Eurosystem favorisiert zur Verwirklichung der Integration des europäischen Binnenmarktes für den Zahlungsverkehr keine spezifische Lösung. Es wird nicht in den Marktwettbewerb zwischen den verschiedenen Systemen, Finanzzentren oder Bankengruppen eingreifen, um die Integration voranzutreiben. Das Ziel besteht in der Gewährleistung gleicher Wettbewerbschancen für die Anbieter von Dienstleistungen im Zahlungsverkehr. Mit diesem Vorgehen kann die Effizienz auch dadurch gefördert werden, dass innovative neue Akteure die Möglichkeit bekommen, ihre effizienten Technologien am Markt einzusetzen.[861]

Deutsche Bundesbank

Der gesetzliche Auftrag der Deutschen Bundesbank ist in § 3 Bundesbankgesetz formuliert: Sie „sorgt für die bankmäßige Abwicklung des Zahlungsverkehrs im Inland und mit dem Ausland und trägt zur Stabilität der Zahlungs- und Verrechnungssysteme bei". Eine Formulierung, die dem EZB-Auftrag sehr nahe kommt. Stark führt aus, was die Bundesbank in ihrem Selbstverständnis im Hinblick auf ihren Auftrag an Aufgaben zu übernehmen hat:[862] Die Überwachungsfunktion besteht in der Schaffung solider Rahmenbedingungen für den Zahlungsverkehr. Sicherheit und Effizienz sind auch hierbei wieder die zentralen Ziele, die es zu erreichen gilt. Das Vorgehen der Bundesbank ist von Kooperation mit der Kreditwirtschaft gekennzeichnet – Stark spricht von der Rolle der Bundesbank als „Bank der Banken"[863]. Der Zahlungsverkehr wird zudem als Kerngeschäft der Bundesbank verstanden, zum einen, um geldpolitische Maßnahmen durchzuführen, zum anderen, um über wettbewerbsfähige Dienstleistungen einen effizienzfördernden Wettbewerb der Branche voranzubringen.

Fabritius formuliert Rolle und Ziele der Zentralbanken 2003 ein wenig nuancierter. Er betont ebenfalls die Aufgabe, sicheren und effizienten Zahlungsverkehr zu fördern. Allerdings sieht er als zentrale Punkte zukünftiger Zentralbankarbeiten die Notwendigkeit, die Überwachungsfunktion zu stärken, und sich aus der Betreiberposition, sofern sie nicht zentrale Aufgabenbereiche wie das finale Settlement der Zahlungen in TARGET2 berührt, zurückzuziehen.[864] In anderen Ländern, beispielsweise Frankreich sind Schritte in diese Richtung im Zahlungsverkehr bereits realisiert worden. Dort ist die Banque de France nunmehr gesetzlich verpflichtet und mit zusätzlichen Befugnissen ausgestattet, die Sicherheit aller Zahlungssysteme („all instruments which, irrespective of the medium or technical procedure used, enable any person to transfer funds"[865]) zu gewährleisten.[866]

[859] Vgl. EZB (2000b), S. 2.
[860] Vgl. EZB (2003a), S. 78.
[861] Vgl. EZB (2002b), S. 62.
[862] Vgl. Stark (2001), S. 4 f. Auch Fabritius (2001), S. 3f. betont die Kooperationswilligkeit der Bundesbank.
[863] Stark (2001), S. 4.
[864] Vgl. Fabritius (2003a).
[865] Beau (2002), S. 6.
[866] Beau (2002), S. 5f.

Die Schnittmenge der obigen Ausführungen ermöglicht es, die vier wesentlichen Ziele der Regulierung im Zahlungsverkehr zu identifizieren:[867]

1) Der Wettbewerb soll zum Wohl der Endverbraucher gesichert werden,
2) Die Effizienz des Systems soll sichergestellt werden, um die volkswirtschaftlich kostengünstigste Lösung zu erhalten,
3) Kooperationen sollen gefördert werden, um reibungslose Abläufe und zahlreiche Funktionalitäten im System zu erreichen, und
4) systemische Verlässlichkeit der Systeme soll erreicht und erhalten werden, um das Vertrauen in den Zahlungsverkehr auf hohem Niveau zu belassen.

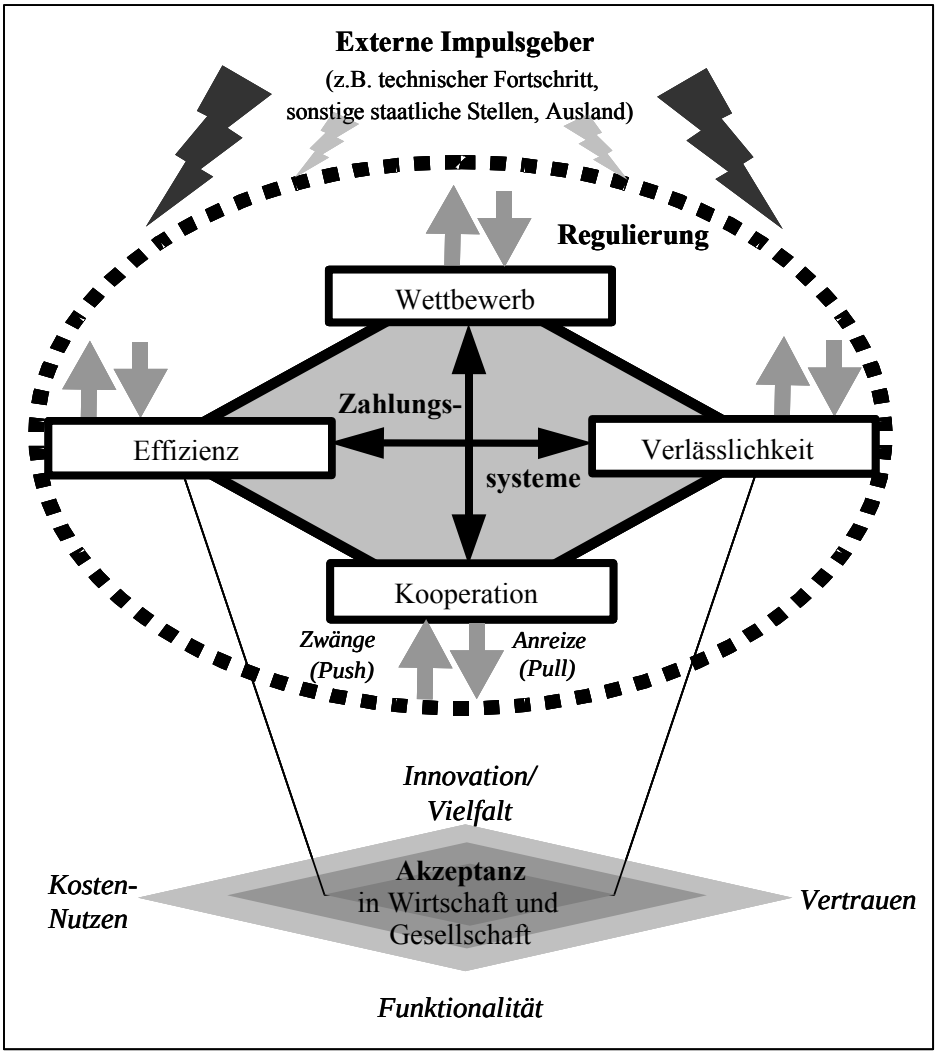

Abbildung 32: Das „Rautenmodell" zur zielführenden Gestaltung von Regulierungsmaßnahmen[868]

Im Rautenmodell (siehe Abbildung 32) finden sich diese vier Ziele in den Eckpunkten einer Raute wieder. Eine Raute wurde als Form gewählt, da die Idealannahme des Modells davon ausgeht, dass a) alle vier Ziele in gleichem Maße erfüllt werden können, und b) jeweils die beiden gegenüberliegenden Punkte auf der Raute korrespondieren. Wettbewerb und Kooperation sind ein Gegensatzpaar, in dem sich Netzwerkgüter, und als solches kann der Zahlungs-

[867] Das Rautenmodell und dessen Herleitung wurde bereits in dieser Form in Hartmann (2003) entwickelt. Es wird der Argumentationslinie von Hartmann und Stroborn folgend im Kontext der vorliegenden Arbeit erweitert.
[868] Hartmann (2003), Abbildung 5, geringfügig modifiziert.

verkehr betrachtet werden, behaupten müssen.[869] Die Nutzung einer nationalen und supranationalen Infrastruktur ist effizient nur über Kooperationsmodelle möglich. Im Gegensatz zu anderen Netzwerk-Gütern – Telekommunikation, Energie, Verkehr – hat im Zahlungsverkehr schon lange ein Wettbewerbsmarkt, wenngleich zu besonderen Bedingungen, existiert. Der Wettbewerb erhält die Innovationskraft der Branche, sorgt für eine Vielfalt der angebotenen Verfahren, und lässt somit den Anwendern die Autonomie ihrer Entscheidung. Das andere Gegensatzpaar sind Verlässlichkeit und Effizienz. Ein grundsätzliches Dilemma von Sicherheit im weitesten Sinne ist es, dass zusätzliche Sicherheit (steigende) Kosten verursacht (siehe Abbildung 23). In diesem Spannungsfeld muss sich auch der elektronische Zahlungsverkehr behaupten. In der Realität kann es durchaus passieren, dass vom Idealbild der Raute nicht mehr viel zu erkennen ist. Dies ist dann der Fall, wenn die Regulierer (gepunktete Ellipse um die Zielraute), die selbst wiederum externen Impulsen, z. B. technischem Fortschritt oder ausländische Entwicklungen, ausgesetzt sind, unterschiedlichen Druck auf die vier Ziele ausüben können, müssen oder wollen. Druck wirkt im Modell in zweierlei Hinsicht. Zum einen wird durch das Regulierungs-Instrumentarium Druck auf den Zahlungsverkehrsmarkt und die vier Eckpunkte ausgeübt (Push-Pfeile), zum anderen werden die Gestaltungsspielräume der Akteure im Markt bei entsprechenden Regularien größer (Pull-Pfeile).

Welche Annahmen stecken ferner im Bild des Rautenmodells? Die Ziele der Regulierung sind für den Zahlungsverkehr nicht als Selbstzweck definiert. Der Zahlungsverkehr hat volkswirtschaftliche Aufgaben zu erfüllen. Im Rautenmodell wird dies durch die Projektion der Raute auf die darunterliegende Raute „Gesellschaft und Wirtschaft“ verdeutlicht. Die einzelnen Ziele der Raute erfüllen in Bezug auf die Akzeptanz und Zufriedenheit der Gesellschaft im Allgemeinen und der Wirtschaft im Besonderen jeweils spezifische Bedürfnisse. Freier Wettbewerb ermöglicht es, die Innovationskraft der Branche zu erhalten. Kooperationen innerhalb des Zahlungsverkehrs – sowohl zwischen Wettbewerbern als auch mit Regulierern – ermöglichen es erst, die Funktionalitäten der Zahlungsinstrumente im Netzwerk auszuschöpfen. Wird Verlässlichkeit erzielt, ist Sicherheit der Zahlungsverkehrssysteme gegeben, dann ist das notwendige Vertrauen zu ihrem Einsatz im Wirtschaftsgeschehen vorhanden. Ökonomische Effizienz spiegelt sich wider in einem aus Sicht der Akteure vernünftigen Kosten-Nutzen-Verhältnis. Eines der Argumente der Deutschen Bundesbank bei ihrer Stellungnahme zum neuen EU-Rechtsrahmen im Zahlungsverkehr lautete dahingehend, die Vielfalt im Zahlungsverkehr, die sich national findet, zu erhalten und nicht regulatorisch einzudämmen, da nur in diesem Fall die Akteure freie Wahl hätten, das ihren Bedürfnissen (Kosten-Nutzen-Relation) entsprechende Zahlungsinstrument zu verwenden.[870]

Stehen die übergeordneten Ziele einer sektorspezifischen Regulierung fest, oder herrscht gesamtgesellschaftlich/europäisch/international – Konsens über diese Ziele, stellt sich die Frage, wie weit Regulierung gehen sollte, auf zwei Ebenen. Zunächst ist das Ausmaß regulierter Bereiche abzuklären, und in einem nächsten Schritt die Tiefe der Regulierung in einem bestimmten Bereich. Die Spanne regulatorischer Möglichkeiten reicht dabei von normativen, qualitativen Aussagen hin zu quantitativen Forderungen im Detail. Dewatripont und Tirole sehen ein Nebeneinander unregulierter und regulierter Bereiche im Finanzsektor als unkritisch an, wenn der betroffene Konsument oder Haushalt in der Lage ist, die mit einem Produkt verbundenen Risiken realistisch einzuschätzen und abzuwägen, ob für ihn ein reguliertes oder unreguliertes Produkt vorteilhafter ist. Die Beurteilung dieser „Mündigkeit“ des Konsumenten ist eng verknüpft mit der Frage, inwieweit sich Informationsasymmetrien – zentrales Argument der Regulierung – messen oder einschätzen lassen. Bei größeren Risiken,

[869] Die Anlehnung an das „magische Viereck“ ist gewollt. Mit der Raute wird lediglich der Wunsch nach Gleichwertigkeit der Ziele stärker betont.
[870] Vgl. Deutsche Bundesbank (2002), Punkt 2, S. 1f. und Antworten auf Frage 49-50, S. 12f.

die in volkswirtschaftlich bedeutende Dimensionen führen, gerät ohnehin der Staat in die Rolle der letztinstanzlichen Versicherung (insurer of last resort).[871] Die Herausforderung für den Regulierer kann in der Folge darin bestehen, diese Risiken für den Staat zu minimieren.

Eine Möglichkeit, das Ausmaß der Regulierung eines Wirtschaftssektors festzulegen, kann in der Abschätzung des Schadenspotenzials der davon betroffenen Akteure (Konsument, Intermediär, Unternehmen) liegen. Es konnte im Rahmen dieser Arbeit herausgearbeitet werden, dass die systemischen Risiken die dem Zahlungsverkehr innewohnen, auf jeden Fall ein, im Vergleich zu anderen Wirtschaftssektoren, hohes Maß an Regulierung benötigen.

Sind die Ziele bestimmt, und das Ausmaß der Regulierung annähernd bekannt, muss in einem nächsten Schritt überprüft werden, welche Regulierungsform, privat, hoheitlich oder Mischformen, im jeweiligen Kontext die effizientere ist. Dennig kommt bei der Analyse des europäischen Zahlungsverkehrs zu der Schlussfolgerung, dass es bislang kaum Erkenntnisse über mögliche Netzwerkeffizienzen in den Bereichen der Kombination von Regulierung mit Markt und Wettbewerb gibt.[872] Anhand des Rautenmodells lassen sich einige der gängigen Argumentationsmuster, greifbarer als bisher möglich, diskutieren.

6.3.2 Die Regulierer im Rautenmodell: Aufgabenteilung und Koordination

Im Rautenmodell sind zunächst weder die Regulierungsform noch die Position der regulierenden Institutionen ersichtlich. Bereits die Herleitung der Ziele, die im Rautenmodell die Eckpunkte darstellen, hat die Schwierigkeiten harmonisierter Regulierungsbemühungen zumindest auf EU-Ebene verdeutlicht: Alle wesentlichen Regulierer positionieren sich auf allen vier Ecken der Raute. Nur in Ansätzen sind bislang klare Positionierungen in der einen oder anderen Ecke erkenntlich, die demzufolge genutzt werden können, um einer Institution koordinierende Funktionen im Regulierungsprozess zusprechen zu können.

Die politischen Entwicklungen in Europa, insbesondere die Bildung der Gemeinschaftswährung, hat für die Regulierungsinstitutionen sichtbare Konsequenzen. Es kommt sukzessive zu einer „Machtverschiebung“, die von „unten“ nach „oben“ läuft. Auf der Ebene einzelner Finanzinstitute wird der Entscheidungsspielraum durch zunehmende Regulierung geringer – es sei denn, die Verwendung institutseigener Risikomanagementverfahren nach Basel II setzt sich umfassend durch. Die Umstrukturierung der europäischen Finanzlandschaft wird institutionell unter anderem durch die Bildung des EPC betont. In Rekordzeit hat die Branche eine potenziell schlagkräftige Instanz der Selbstregulierung aufgestellt, die für die hoheitlichen Regulierer ein wichtiger Ansprechpartner sein wird. Je durchsetzungsfähiger allerdings das EPC, umso geringer die Durchsetzungskraft des Einzelnen, da bei Kompromissen im Entscheidungsfindungsprozess analog zum deutschen ZKA-Vorgehen jeder Einzelne zunächst auf nationaler Ebene und anschließend auf europäischer Ebene Zugeständnisse machen muss.

Eine analoge Entwicklung ist bei den Institutionen der Aufsicht zu beobachten. Die auf europäischer Ebene im Rahmen des FSAP beschlossene Vereinheitlichung des europäischen Binnenmarkts für Finanzdienstleistungen wird nur durch mehr Regulierungsgewalt der supranationalen Institutionen zu realisieren sein. Dementsprechend fällt die empfohlene Wahl der Rechtsinstrumente eines neuen Rechtsrahmens für den Zahlungsverkehr im Binnenmarkt

[871] Dewatripont (1994), S. 34 f. Auch die Deutsche Bundesbank argumentiert in einer Stellungnahme zum Entwurf des neuen EU-Rechtsrahmens für den Zahlungsverkehr in diese Richtung. Hinreichende Transparenz würde Regulierung in letzter Instanz minimieren (vgl. Deutsche Bundesbank (2002b), Punkt 2, S. 1). Gleichwohl gilt die Frage, wie eine solche Transparenz hergestellt werden kann, als ungelöst.
[872] Vgl. Dennig (2002), S. 111.

– teils von den Marktteilnehmern explizit gefordert – auf EU-Verordnungen, die nationales Recht ersetzen und keinen Umsetzungsspielraum für nationale Gesetzgeber lassen.[873] Die Geschwindigkeit dieser Machtverschiebung ist jedoch institutionell von der Aufsicht nicht mitgegangen worden. Es fehlt auf europäischer Ebene eine dem BAFin vergleichbare Institution, die aufsichtliche Fragestellungen einheitlich definieren und überprüfen kann. Diese Aufgabe kann nur zum Teil von der EZB übernommen werden, zumindest solange die in Deutschland gepflegte Aufgabenteilung zwischen Deutscher Bundesbank und BAFin als Erfolg gesehen wird.

Die Forderung nach der Identifizierung relevanter Ziele und einer an diese angepaßten Aufgabenteilung wird von den Zentralbanken selbst in den „Core Principles for Effective Banking Supervision" gestellt:[874] „An effective system of banking supervision will have clear responsibilities and objectives for each agency involved in the supervision of banking organisations." Die Darstellung der für die Sicherheit im Zahlungsverkehr und der IT-Infrastruktur zuständigen Institutionen und Regelwerke in den Abschnitten 4.4 und 5.1 lässt die Problematik der BIZ-Forderung nach einer solchen effektiven Aufgabenzuweisung und -teilung deutlich werden, insbesondere wenn, wie es im europäischen Kontext der Fall ist, nicht „nur" länderspezifische, sondern zusätzlich supranationale Besonderheiten berücksichtigt werden müssen. In den vorbereitenden Sitzungen zur Neugestaltung des europäischen Rechtsrahmens im Zahlungsverkehr wird in der Stellungnahme der Deutschen Bundesbank diese Problematik explizit betont: Die Bundesbank steht einer weitreichenden Harmonisierung nationaler Rechtskonstrukte im Zahlungsverkehr äußerst skeptisch gegenüber und verweist auf das Subsidiaritätsprinzip der EU.[875] Werden die Ziele der Regulierer nicht gefährdet, plädiert die Bundesbank für das Beibehalten nationaler Besonderheiten. Die Bundesbank möchte im Kern (und im Sinne des Rautenmodells) die Vielfalt im nationalen Zahlungsverkehr, der durch innovative Produktentwicklungen geprägt ist, weitgehend erhalten wissen, und sieht die Gefahr, dass durch europaweit einheitliche Regelungen „gut funktionierende und von Marktteilnehmern akzeptierte Verfahren auf nationaler Ebene unmöglich gemacht werden."[876] In der Konsequenz führt diese Haltung letzlich zu einem „Machterhalt" nationaler Regulierungsinstitutionen.

Die einzelnen europäischen Zentralbanken nehmen innerhalb des Rautenmodells bereits durchaus unterschiedliche Positionen ein. Während die Deutsche Bundesbank sich bei der Überwachung der Sicherheit von elektronischen Zahlungssystemen weitestgehend auf Großsysteme beschränkt, und erst in Ansätzen von einer notwendigen eingehenderen Betrachtung der Sicherheit von Retail-Bezahlverfahren die Rede ist,[877] geht die französische Zentralbank sehr viel offensiver vor. Mit dem sogenannten „Everyday Security Act" wurde die Banque de France durch einen neuen Artikel L141-4 des „Financial and Monetary Code" in ihrer Aufsichtsrolle gestärkt:[878] „The Banque de France shall ensure the security of means of payment, other than banknotes and coins, as defined in Article L311-3, and the relevance of the standards applicable thereto. If it deems that any such means of payment is insufficiently secure, it may recommend that the issuer take all necessary measures to remedy such insufficiency. If its recommendations are to no avail, it may, after having solicited the observations of the issuer, hand down a negative opinion published in the Official Journal." Eine solchermaßen angedrohte Sanktion durch die Aufsicht ist ein starkes Druckmittel. Die

[873] Vgl. KOM (2003b), S. 17f.
[874] Vgl. BIZ (1997), S. 4 und 13 f.
[875] Vgl. Deutsche Bundesbank (2002b), S. 1 f.
[876] Deutsche Bundesbank (2002b), Punkt 3, S. 2.
[877] Vgl. Fabritius (2003a).
[878] Beau (2002), S. 5 f.

französische Zentralbank formuliert ihre Aufsichts-Ziele im Hinblick auf sichere Zahlungssysteme auch im B2C-Bereich dementsprechend weitreichend:[879]

- Relevante Bedrohungen für einzelne Systeme sollen identifiziert werden.
- Ein Mindestmaß an Sicherheit wird von der Zentralbank definiert und gefordert.
- Die Zentralbank überwacht kontinuierlich die Systeme, um die Wahrung der Sicherheitsziele zu gewährleisten.

Leitsatz für die Banque de France ist dabei, die Sicherheit von Zahlungssystemen in offenen Netzen deutlich zu erhöhen, das Vertrauen der Konsumenten in diese Systeme zu gewinnen oder zu erhöhen, und gleichwohl noch betriebswirtschaftlich rentable Systeme zu erhalten. Ein Grund für das verstärkte Engagement der Aufsicht im B2C Bereich sind Untersuchungen, die zum Ergebnis geführt haben, dass zwei Drittel der Konsumenten in Frankreich aus Angst vor fehlender Sicherheit nicht im Internet einkaufen und bezahlen wollen.[880] Mit ihrer klaren Haltung positioniert sich die französische Nationalbank im Rautenmodell auf dem Zielpunkt der Verlässlichkeit der Systeme.

Die Deutsche Bundesbank ist im Europäischen System der Zentralbanken die Betreiberin des größten nationalen Zahlungssystems RTGS^{plus}. Im deutschen Gironetz nimmt sie als Gironetzbetreiber gleichfalls eine wichtige Rolle ein. Ein Vorteil dieser Position ist eine sehr enge Marktbeobachtung, sowohl in Bezug auf Sicherheitsfragen im elektronischen Zahlungsverkehr, als auch im Hinblick auf die Kosten und Preisgestaltung. Indem die Deutsche Bundesbank, die Preise ihrer angebotenen Dienstleistungen im Zahlungsverkehr, innerhalb der gebotenen Kostendeckung und in Absprache mit der EZB, frei setzen kann, verfügt sie über einen wichtigen Hebel für die Durchsetzung des Effizienzziels. Indirekt bestimmt die Zentralbank mit ihrem Angebot Akzeptanz und Verbreitung elektronischer Zahlungsinstrumente.[881] Im Rautenmodell lässt sich die Position der Bundesbank schwieriger eindeutig bestimmen, in Einzelbereichen werden alle vier Ziele stringent verfolgt. Dennoch kann es innerhalb eines europäischen Harmonisierungsprozesses schwierig werden, wenn eine Institution keine sichtbar dominante Position im Rautenmodell besetzt. Vor diesem Hintergrund mag es zu verstehen sein, dass Fabritius die Bundesbank verstärkt in der Überwachungsfunktion und weniger in der Betreiberrolle verankert sieht.[882]

Unterschiedliche Positionen nationaler Zentralbanken sind in einer Übergangsphase vorstellbar, sollten aber, falls das „level playing field"-Argument greift, in dem für alle Marktteilnehmer europaweit gleiche Bedingungen gefordert werden, konsolidiert werden. Zu diesem Zweck bietet sich als Vermittler die EZB (unterstützt von der Europäischen Kommission) an, die versuchen sollte, die Positionierung des ESZB innerhalb des Rautenmodells zu bestimmen. De jure ist sie dazu bereits befugt. Artikel 105 (4) des Vertrags und Artikel 4 der Statuten legt fest, dass die nationalen Zentralbanken die EZB konsultieren müssen, sobald Vereinbarungen auf nationaler Ebene die Belange der EZB berühren. Angesichts der personellen Überlegenheit der nationalen Zentralbanken im ESZB wäre es durchaus denkbar, dass einzelne Zentralbanken im Sinne von Kompetenzzentren agieren. Politisch ist ein solch dezentralisierter Ansatz auf jeden Fall erheblich leichter umzusetzen als der Versuch, auf Seiten der EZB zusätzliche personell unterlegte Kompetenzen zu Lasten der nationalen

[879] Vgl. Beau (2002), S. 6.
[880] Beau (2002), S. 3. Auch bei einer von der EU-Kommission in Auftrag gegebenen Studie liegt das Vertrauen der französischen Verbraucher in elektronische Zahlungsverkehrsinstrumente im unteren Mittelfeld, vgl. EU (2003), Tabelle zum Vertrauensindikator.
[881] Vgl. EZB (2001a), S. 129 f.
[882] Vgl. Fabritius (2003a).

Zentralbanken aufzubauen. Ein solches Vorgehen kann auf die im Zuge der Bildung des ESZB gegründeten und mittlerweile etablierten Koordinierungsgremien auf verschiedensten Ebenen zwischen nationalen Zentralbanken und der EZB aufbauen.

Die Schwierigkeiten einer konsistenten Regelsetzung hatte jedenfalls die Europäische Kommission bei ihrem Versuch, einen neuen Rechtsrahmen für den Zahlungsverkehr im Binnenmarkt zu formulieren, vor Augen. Nicht nur sollen die Rechtsvorschriften technisch neutral formuliert werden, sondern – als Leitprinzip wurde mit gewisser Ironie formuliert: „Die Überarbeitung der Rechtsvorschriften für den Zahlungsverkehr muss zusätzlichen Nutzen bringen“.[883]

Überlegungen zu einer konstruktiven Arbeitsteilung zum optimalen Erreichen der verfolgten Ziele im Sinne des Rautenmodells sollten zwei Aspekte berücksichtigen:

1) Wie ist das Zusammenspiel der verschiedenen Regulierer, private und staatliche, supranationale, mit den Marktteilnehmern? Welche Organisationsform der Regulierung und Aufsicht wird gewählt - zentral versus dezentral, bzw. national versus supranational?
2) Die Granularität von Regelungen: Welchen Detaillierungsgrad haben Regulierungen auf welcher hierarchischen Stufe der Regulierung?

Ansätze zur Lösung des ersten Aspekts zeigen sich auf nationaler Ebene. Der Kooperationsgedanke wird ausgebaut: Bei der BAFin mit der Überlegung, einen Fachbeirat zur sinnvollen Auslegung der mit zahlreichen Öffnungsklauseln versehenen MaK zu gründen.[884] In § 8 Abs. 1 und Abs. 2 FinDAG wird ein Fachbeirat institutionalisiert, der die Bundesanstalt bei der Erfüllung ihrer Aufgaben beraten soll und Empfehlungen zur allgemeinen Weiterentwicklung der Aufsichtspraxis einbringen kann. Die 24 Mitglieder werden vom Finanzministerium bestellt und sollen die Finanzwissenschaft, die Kredit- und Versicherungswirtschaft, die Deutsche Bundesbank und die Verbraucherschutzvereinigungen repräsentieren.[885]

Der aufgezeigte Trend zu qualitativen Normen führt zunehmend zu Kommunikationsproblemen zwischen Aufsicht und Markt. Ein Fachbeirat erscheint als ein möglicher Weg, in kooperativer Form flexible Lösungen für die Interpretation von Vorgaben bis auf prozessualer Ebene zu finden. Dazu braucht es jedoch Zeit. Das bisherige Verhältnis von Kreditinstituten zu Aufsichtsorganen ist von (vorsichtigem) Misstrauen gekennzeichnet. Deutlich wird dies beispielsweise an den Zweifeln der Institute, als die BAFin die MaK mit zahlreichen Öffnungsklauseln versehen hatte. Die Institute begrüßten diese Klauseln, äußerten allerdings Bedenken am Fortbestand der Öffnungsklauseln, die erst im Anschreiben an die Kreditinstitute bei der Versendung des Rundschreibens 34/2002 explizit vom Präsidenten der BAFin zerstreut werden mussten.[886]

Neue institutionelle Strukturen, z. B. ein banken- und aufsichtsübergreifendes Operational Risk Emergency and Analysis Centre wie in Kapitel 5.3.3.4 vorgeschlagen, könnten unter Umständen helfen, das Problem der allgemeinen Anwendbarkeit von Vorgaben bei einer gleichzeitigen Fülle divergenter Systeme zu lösen. Dieses Vorgehen bietet zusätzlich die Chance, das – auch für den in Basel II formulierten Supervisory Review Process – notwendige Vertrauensverhältnis zwischen zwischen Aufsicht und Marktteilnehmern aufzubauen.

[883] KOM (2003b), S. 17.
[884] Vgl. BAFin (2002c) und FinDAG (2002).
[885] FinDAG (2002), § 8 Abs. 1 und Abs. 2.
[886] Vgl. BAFin (2002b).

Welche Organisationsform im Hinblick auf aufsichtliche Institutionen kommt den Bedürfnissen des Marktes für sichere Zahlungsverkehrsdienstleistungen nahe? Diese Frage entscheidet sich unter Berücksichtigung der im zweiten Aspekt so genannten Granularität der Regulierungsvorgaben. Es lassen sich zwei idealtypische Konzepte der Regulierung differenzieren, ein kaskadierender Ansatz (siehe Abbildung 33) und ein vertikaler Ansatz der Regulierung (siehe Abbildung 34).

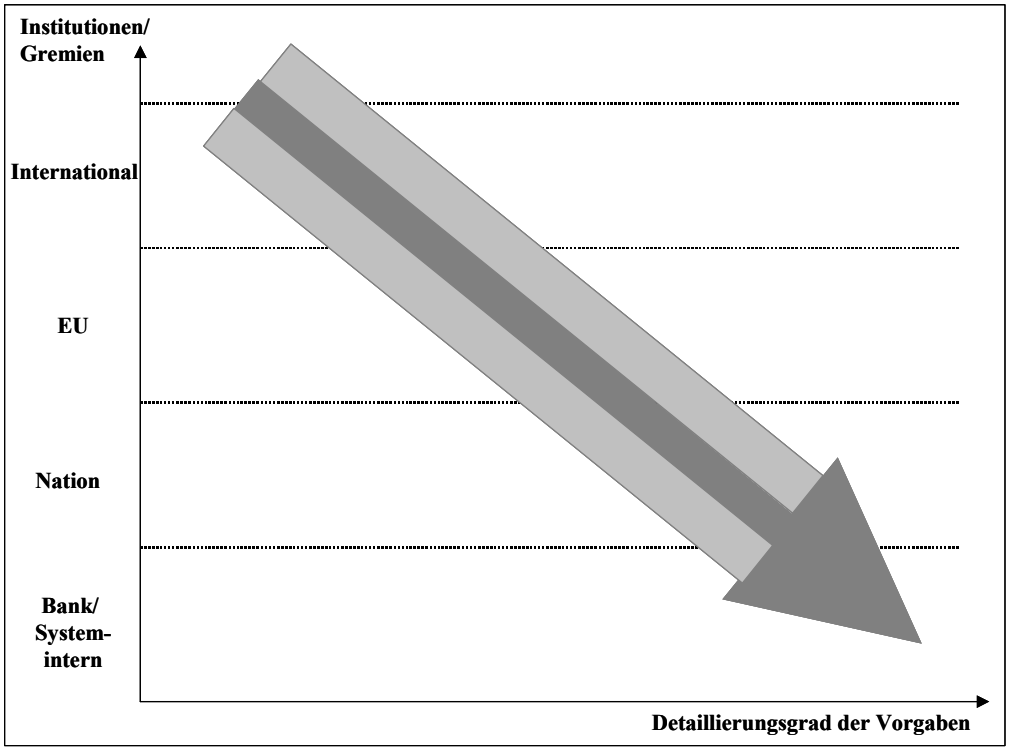

Abbildung 33: Idealtypische Kaskadierung aufsichtsrechtlicher Regelungen: Alternative I

Im ersten Fall, der Kaskadierung aufsichtlicher Regelungen (Alternative I), nimmt die Granularität, die angibt, wie sehr ein Regulierungsinstrument ins Detail geht, mit abnehmender Zentralität, das heißt in Richtung der Unternehmensebene zu. Auf supranationaler Ebene werden lediglich Rahmenbestimmungen erlassen. Im zweiten Fall, dem vertikalen Festlegen aufsichtlicher Regelungen (Alternative II), erfolgt die Feinspezifizierung einer Regelung auf der obersten zentralen Ebene. Ein Beispiel für ein solches Vorgehen stellen die EMSSO der EZB dar, die den folgenden Institutionen wenig Interpretationsspielraum geben, bzw. kaum weitere Detaillierung zulassen. Alternative I findet sich beispielsweise im Risikomanagement realisiert mit ISO-Norm 17799, oder mit den Standards für die Überwachung von Euro-Massenzahlungssystemen der EZB, die bislang sehr allgemein gehalten sind. Und dementsprechend den nachgelagerten Institutionen Spielräume und Detaillierungsmöglichkeiten lassen. Ein Unterscheidungsmerkmal der beiden Alternativen I und II ist die „Lebensdauer“ oder Aktualität von Regularien. Mit zunehmender Detaillierungstiefe sinkt die Verwendbarkeit im Zeitablauf in der Regel. Im kaskadierenden Modell besteht die Möglichkeit von qualitativen Vorgaben, die zeitlich invariater sind, langsam und angepaßt an regionale Besonderheiten die Regularien auf quantitative Detaillösungen dezentral herunterzubrechen. Wird bei Alternative II jeweils auf oberster Ebene detailliert neu angepasst und geregelt, muss aufsichtlich und marktseitig dieser Prozeß jeweils bis auf Unternehmensebene nachvollzogen werden; ein unter Umständen schwieriges Unterfangen.

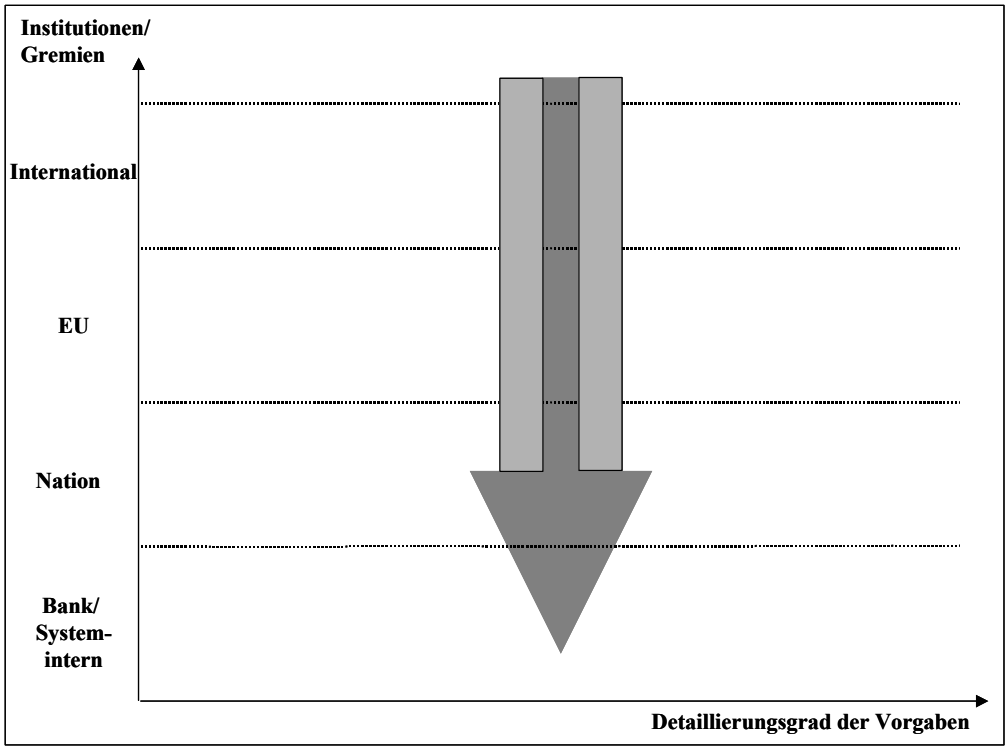

Abbildung 34: Idealtypisches vertikales Festlegen aufsichtsrechtlicher Regelungen: Alternative II

Im ersten Fall, der Kaskadierung aufsichtlicher Regelungen (Alternative I), nimmt die Granularität, die angibt, wie sehr ein Regulierungsinstrument ins Detail geht, mit abnehmender Zentralität, das heißt in Richtung der Unternehmensebene zu. Auf supranationaler Ebene werden lediglich Rahmenbestimmungen erlassen. Im zweiten Fall, dem vertikalen Festlegen aufsichtlicher Regelungen (Alternative II), erfolgt die Feinspezifizierung einer Regelung auf der obersten zentralen Ebene. Ein Beispiel für ein solches Vorgehen stellen die EMSSO der EZB dar, die den folgenden Institutionen wenig Interpretationsspielraum geben, bzw. kaum weitere Detaillierung zulassen. Alternative I findet sich beispielsweise im Risikomanagement realisiert mit ISO-Norm 17799, oder mit den Standards für die Überwachung von Euro-Massenzahlungssystemen der EZB, die bislang sehr allgemein gehalten sind. Und dementsprechend den nachgelagerten Institutionen Spielräume und Detaillierungsmöglichkeiten lassen. Ein Unterscheidungsmerkmal der beiden Alternativen I und II ist die „Lebensdauer" oder Aktualität von Regularien. Mit zunehmender Detaillierungstiefe sinkt die Verwendbarkeit im Zeitablauf in der Regel. Im kaskadierenden Modell besteht die Möglichkeit von qualitativen Vorgaben, die zeitlich invariater sind, langsam und angepaßt an regionale Besonderheiten die Regularien auf quantitative Detaillösungen dezentral herunterzubrechen. Wird bei Alternative II jeweils auf oberster Ebene detailliert neu angepasst und geregelt, muss aufsichtlich und marktseitig dieser Prozeß jeweils bis auf Unternehmensebene nachvollzogen werden; ein unter Umständen schwieriges Unterfangen.

Werden die in Kapitel 4.4 benannten Regulierer und ihre Regulierungsinstrumente in einem Koordinatensystem „Detaillierungsgrad der Vorgaben" gegenüber der „organisatorischen Ebene" abgetragen, ergibt sich zunächst ein Bild gemäß Abbildung 35. Die meisten Regelungen folgen aufgrund ihrer unspezifischen Ausformulierung (noch) dem kaskadierenden Ansatz.

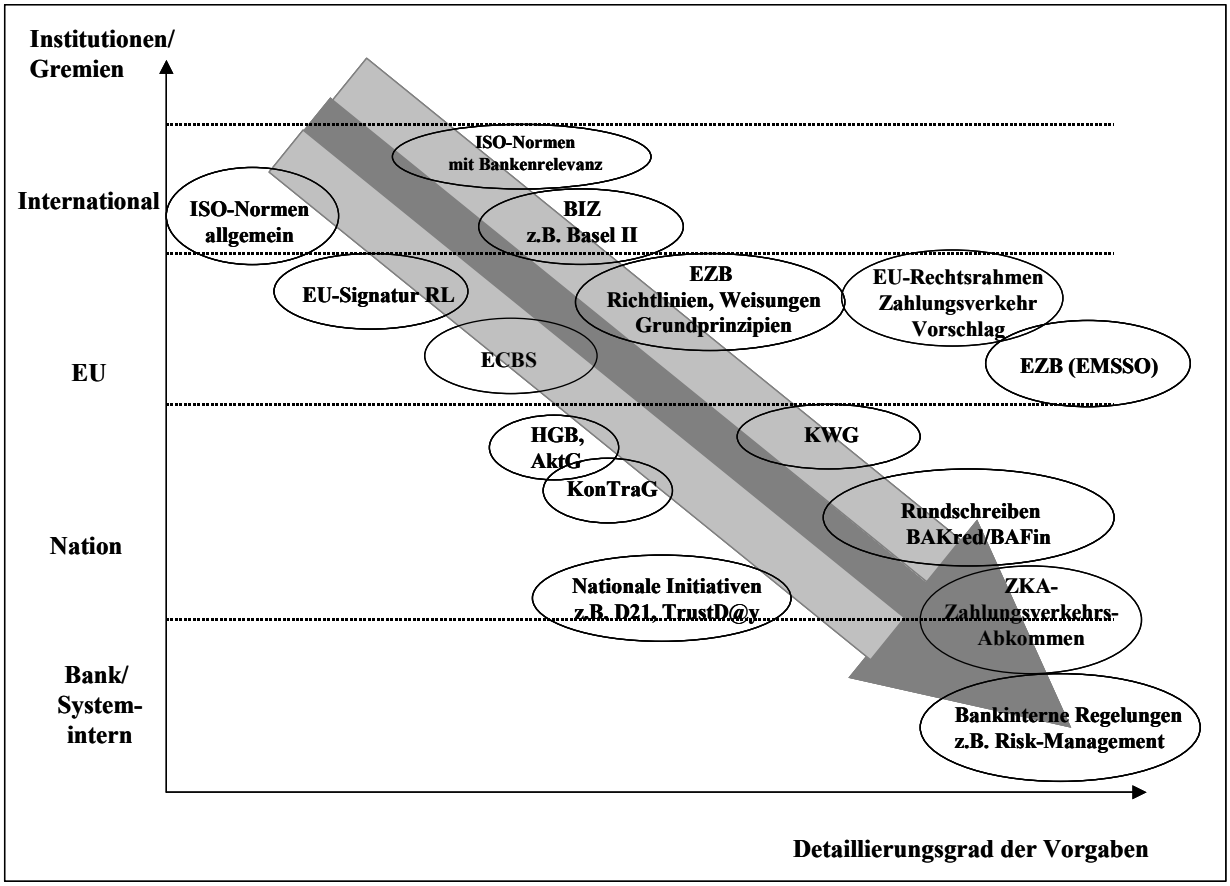

Abbildung 35: Realtypischer Regulierungspfad?

Die jüngsten Entwicklungen auf Seiten der Regulierung lassen einige „Ausreisser“ identifizieren. Namentlich sind dies die bereits erwähnten EMSSO der EZB aber auch die detaillierten Vorgaben für die Verwendung institutsinterner Meßverfahren zur Ermittlung Operationeller Risiken in Basel II, und zusätzlich einige der Verordnungen, die sich im Zuge des EU-Kommissionsvorschlags für einen neuen Rechtsrahmen im europäischen Zahlungsverkehr abzeichnen. Werden diese Ansätze dem vertikalen Regulierungspfad zugeordnet, ergibt sich ein gemischtes Bild der Alternativen I und II: Alternative III in Abbildung 36. Alternative III verdeutlicht die Problematik, in der sich aufsichtliche und regulierende Institutionen befinden.

Mit der Einführung vertikaler Ansätze in etablierte kaskadierende Strukturen, die insbesondere vor der Einführung des ESZB funktioniert haben, wird neben der Frage geordneter Prozeduren der Koordinierung und der Frage nach der aufsichtlichen Überprüfung der resultierenden Vorgaben auch die Machtfrage deutlich: Wer hat und braucht Personal, für welche Aufgaben? Wo ist die Expertise? Können nationale Besonderheiten dann nicht mehr berücksichtigt werden? Diese Frage ist einerseits zutiefst politisch und zieht sich durch den gesamten europäischen Einigungsprozess wie ein roter Faden. Auf der fachlichen Ebene der Sicherheit der Bezahlverfahren muss der Koordinationsprozess optimiert werden, um nicht Unstimmigkeiten im System regulatorisch zu bewirken, die anschließend in Risiken münden.

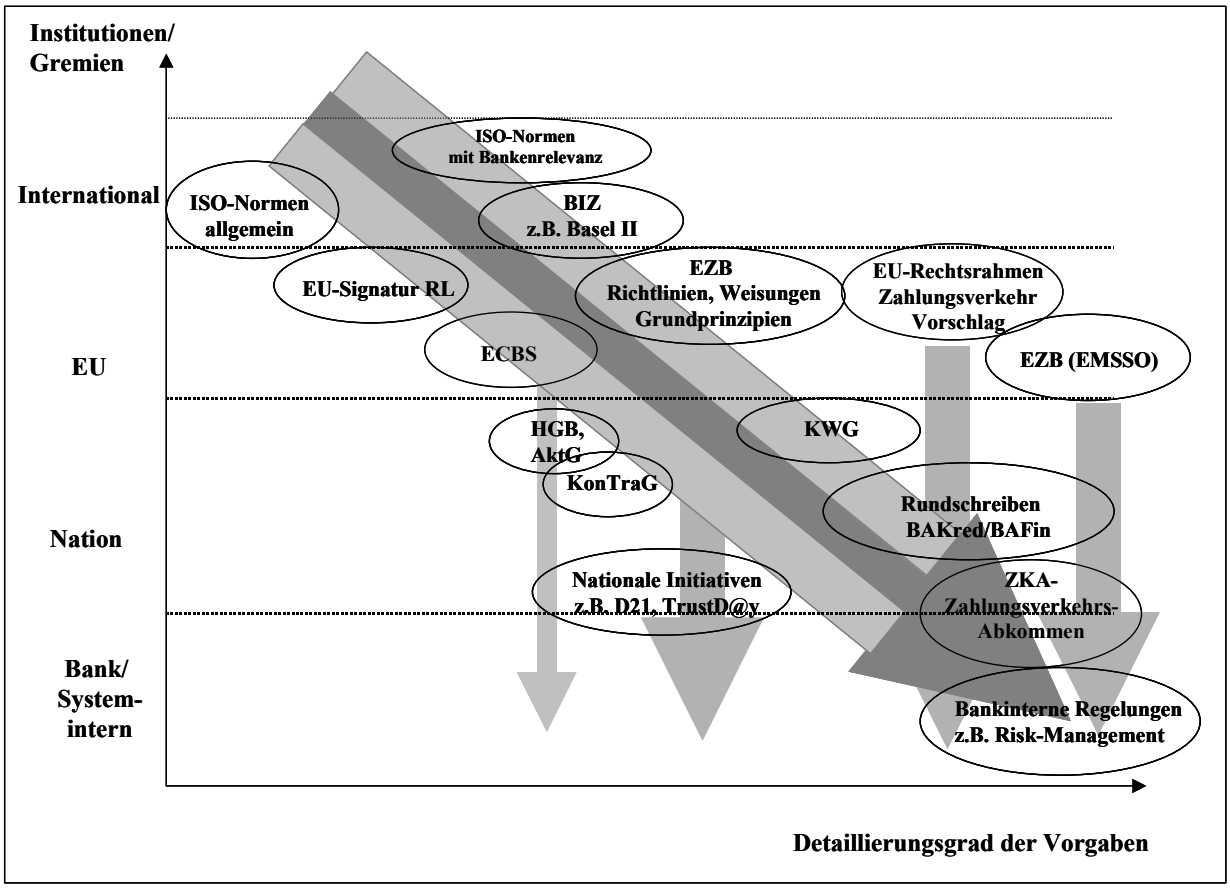

Abbildung 36: Idealtypischer Regulierungspfad: „level playing field"-Alternative III

Die Koordination muss, in Abbildung 36 wird dies anschaulich deutlich, auf und über alle Ebenen horizontal und vertikal stattfinden. Im Idealfall kann parallel vorgegangen werden:

1) Zunächst erfolgt eine horizontale Abstimmung der hoheitlichen Organe der Regulierung, einmal auf bankrechtlicher Ebene (in Deutschland wären dies insbesondere Bundesbank und BAFin), dann auf allgemeiner Ebene (in Europa vor allem E(S)ZB und EU-Kommission). Die Bedarf vertikaler Abstimmung hängt von der politischen Machtverteilung der Ebenen ab (Subsidiarität versus Zentralität).
2) Die privaten Regulierer stimmen sich ebenfalls ab (ZKA, ESBC, EPC aber auch in Bezug auf Standards allgemeine Organisation wie die ISO).
3) Sind die Positionen klar, können staatliche und private Regulierer in den Abstimmungsprozess gehen. Dabei stellt sich die Frage, inwieweit die bisherigen Strukturen ausreichen, oder inwieweit es (nicht nur auf europäischer Ebene) eine institutionalisierte Form des Austauschs geben sollte, die bislang vor allem über die wechselseitige Teilnahme an Arbeitskreisen/Sitzungen gewährleistet ist.
4) Ein wichtiger letzter Schritt umfasst die Abstimmung mit dem Markt, die mittlerweile auf europäischer Ebene zumindest zunehmend in Konsultationsphasen Anwendung findet. Die BIZ betont aufgrund positiver Erfahrungen bei Basel II die Notwendigkeit solcher Konsultationsphasen, die bis hin zu gemeinsamer Erarbeitung neuer Standards führen können, für die zukünftige regulatorische Tätigkeit.[887]

[887] Vgl. BIZ (2003c), S. 15, Ziffer 64.

Deutlich wird bei diesen Überlegungen zu notwendigen Koordinierungsmaßnahmen (nicht nur) im Bereich sicherer elektronischer Zahlungssysteme die Tatsache, dass einzelne Institutionen auf jeder Ebene zentrale Koordinierungsaufgaben übernehmen müssen. Diesen können sie nur nachkommen, wenn sie in einzelnen Bereichen gebündelte Kompetenz erwerben (können). Im Bild des Rautenmodells würde dies beispielsweise bedeuten, dass zwar alle vier Ziele der Regulierung von allen Akteuren mitgetragen werden, aber dennoch die Extrempunkte mit klaren „Führungsrollen" besetzt werden. Denkbar wäre nach den vorangegangenen Ausführungen beispielsweise, dass die EU-Kommission auf Europäischer Ebene den Bereich Wettbewerb besetzt, die EZB die Zuverlässigkeit/Sicherheit der Zahlungssysteme und zum großen Teil auch (in ihrer Eigenschaft als Betreiber zentraler Zahlungssysteme (selbst oder über die NZBs) die Effizienz. Die Kooperationssaufgabe kann zu einem zentralen Teil in die Verantwortung des EPC übergehen.

6.3.3 Regulierungsform

Eine Frage, die insbesondere in Zeiten der Deregulierung häufig diskutiert wird, ist die nach der richtigen Abstimmung hoheitlicher und privater Regulierungsaufgaben.

Ein wesentliches Charakteristikum aufsichtlicher Entwicklungslinien ist der stattfindende Paradigmenwechsel der Aufsichtsprinzipien, der in Basel II seinen vorläufigen Höhepunkt findet. Will man Schlagworte für die Regulierungsdoktrin finden, die im Bereich Sicherheit angewendet wird, so kann von einem Wandel weg von der bisher gepflegten "Security by Obscurity" hin zu "Security by Transparency" gesprochen werden, der notwendigerweise eine veränderte Positionierung im Gefüge Finanzsektor-Aufsicht zur Folge hat.

Der so genannte "Security by Obscurity"-Ansatz basiert auf einem Sicherheitsverständnis des Unternehmens, in dem möglichst wenig über sicherheitsrelevante technische und organisatorische Details nach außen (teils auch nach innen) dringt. Werden nur grobe Finanzkennziffern eines Unternehmens von der Aufsicht beurteilt, einzelne Schadensfälle soweit möglich nicht nach außen kommuniziert, funktioniert dieses Vorgehen in der Unternehmens-Aufsicht-Relation hinreichend gut. Nehmen die systemischen Risiken, wie in den vorigen Kapiteln für den Zahlungsverkehr gezeigt, aus unterschiedlichen Gründen im Zeitverlauf zu, kann das Prinzip problematisch werden. Die Tatsache, dass zu Beginn der Erhebung Operationeller Risiken im Bankensektor durch die BIZ Ende der neunziger Jahre praktisch keine verwertbaren Datensätze verfügbar waren, stützt die These, dass ein "Security by Obscurity"-Ansatz verwendet wurde, empirisch.

Der "Security by Transparency"-Ansatz versucht, sicherheitsrelevante Prozesse einem klar vorgegebenen Schema gemäß zu behandeln, beispielsweise in Anlehnung an das Risikomanagement nach ISO 17799. Verantwortungen für (IT-)Sicherheit werden klar definiert und bis in die Unternehmensleitung verankert. Gleichwohl bedeutet ein solches Vorgehen nicht, alle Sicherheitsmaßnahmen eines Unternehmens offenzulegen. Die höchste Robustheit liegt vermutlich bei Ansätzen, die ein funktionierendes Risikomanagement etabliert haben und zusätzlich die technischen und organisatorischen Sicherheitsmaßnahmen so abgestimmt haben, dass selbst für potenzielle Innentäter nie sicher ist, welche Maßnahmen im Schadensfall greifen. Ein exellentes Beispiel im Zahlungsverkehr ist der bereits zitierte Schadensfall, bei dem ein betrügerischer Millionentransfer ins Ausland über Korrespondenzbankbeziehungen misslang, da dem (Innen-)Täter ein internes Limit, welches einen Kontrollanruf auslöste, nicht bekannt war.[888]

[888] Vgl. Thodén (1999), S. 67.

Die in Basel II ausgelösten Prozesse qualitativer Aufsichtsvorgaben, die um die Überprüfung quantitativer bankinterner Verfahren ergänzt werden, erfordern transparente Maßnahmen im Bereich Risikomanagement. Diese sind unabdingbare Voraussetzung für eine Verschiebung hoheitlicher Regulierung und Aufsicht hin zu einem Ansatz, der von Selbstregulierung der Finanzdienstleister ausgeht.

In Europa wie in den USA finden sich zunehmend Aussagen wie die von Anthony Santomero, Präsident der Federal Reserve Bank of Philadelphia[889]: „The private sector is encouraged to be proactive in self-regulating." Diese Aufforderung zu vermehrter Selbstregulierung durch die Wirtschaft wird ergänzt um die Diskussion nach den möglichen Formen der Kooperation staatlicher und privatwirtschaftlicher Regulierungsorgane. William McDonough formuliert den Anspruch des US-amerikanischen Zentralbankensystems: „In these cooperative efforts with the private sector to improve the payment system, the central bank often brings to the table a broad overview of the payment system that may not always be apparent to those people deeply involved in the day-to-day details. Central banks can often provide the necessary leadership by:

- serving as catalysts for constructive change and contingency planning; and
- enccouraging cooperation, even among competitors, to achieve goals that benefit the payments industry as a whole."

Die deutsche Lösung in diesem Bereich, die von der Kooperation eines bankeneigenen Regulierungsgremiums ZKA mit der Deutschen Bundesbank und der BAFin geprägt ist, kommt dem US-Anspruch sehr nahe. Es wurde in der Diskussion über die strategische Positionierung der Akteure im Finanzsektor in Deutschland allerdings deutlich, dass Zahlungsverkehr und -dienstleistungen nicht mehr länger ausschließlich im Bankensektor angesiedelt sind. Gibt es jedoch nicht nur einen Ansprechpartner wie den ZKA für die Regulierer, kann der Koordinationsprozess schwierig werden, da vielfach von Entscheidungen auch einander widersprechende Wettbewerbsbelange der einzelnen Akteure berührt sind, die zudem alle in ähnlicher Weise organisiert sein sollten. Ist nur eine Branche Verhandlungspartner der Regulierer, beispielsweise im ZKA die Banken und Sparkassen, gibt es noch immer hinreichend Friktionen innerhalb des Gremiums. Gleichwohl kann ein gefundener Kompromiss auch dazu dienen, außenstehende Wettbewerber vom Markt fernzuhalten, oder den Markteintritt zu erschweren.

Die Vorteile der kontrollierten Selbstregulierung sind jedoch unbestritten. Beispielsweise kann bei einer branchenweiten Selbstregulierung, z. B. im ZKA, eine steilere Lernkurve im Hinblick auf systemische Risiken vermutet werden. In diesem Fall können Lernerfahrungen, die in entsprechenden Gremien und Arbeitsgruppen, kommuniziert werden, manch eine Regulierungsmaßnahme ersetzen oder verhindern. Beispielsweise gibt es bei ZKA und EPC für unterschiedlichste Themenfelder rund um Sicherheit im Zahlungsverkehr zuständige Arbeitsgruppen.[890] In der Folge plädieren verschiedene Autoren für eine Harmonisierung europäischer Aufsichts- und Regulierungsstrukturen, die an das deutsche Modell angelehnt sind. Es wird sowohl die Notwendigkeit einer europäischen Finanzaufsicht als auch eines europäischen ZKA festgestellt.[891]

Inwieweit nationale Strukturen der Selbstregulierung auf europäischer Ebene als Blaupause dienen können, hängt wesentlich von der Einigungskraft innerhalb der Branche ab, keine leichte Aufgabe angesichts unterschiedlichster Strukturen der Bankenlandschaft in Europa.

[889] Sienkiewicz (2002), S. 3.
[890] Vgl. für den EPC BdB (2003b), Abb. 19, S. 57.
[891] Vgl. Kern (2003), Schmidt (2001), Rehm (2001) sowie Walkhoff (2001).

Andererseits wird für die Aufsicht auf europäischer Ebene die Möglichkeit, ein „level playing field“ über Selbstregulierung und internen Druck der Branche zu realisieren, ein starker Motor für derartige Konzepte sein. Nicht zu unterschätzen ist die Notwendigkeit einer Vertrauensbasis, die zwischen hoheitlichen Regulierern/Aufsicht und Geschäftsbanken und den jeweiligen Gremien vorhanden sein muss. Selbst in Deutschland, geprägt von guten Erfahrungen im Zusammenspiel von ZKA und Deutscher Bundesbank, finden sich in der Innenschau kritische Aussagen wie die von Fabritius, der die Notwendigkeit kooperativer Ansätze betont, aber im Rückblick Defizite am Beispiel der Integration der Deutschen Bundesbank in die Arbeiten zur Sicherheit der GeldKarte im ZKA aufzeigt.[892]

In den Konsultationen zu Basel II zeigt sich eine mögliche Lösung für die Überwindung von Vertrauensdefiziten zwischen Zentralbanken und Aufsicht auf der einen und Geschäftsbanken auf der anderen Seite:[893] „Supervisors will review the capital requirement produced by the operational risk approach used by a bank (wether Basis Indicator, Standardised Approach or AMA) for general credibility, especially in relation to a firm’s peers. In the event that credibility is lacking, appropriate supervisory action under Pillar 2 will be considered.” Auf der operationalen Ebene der Unternehmung können qualitative Vorgaben in Kombination mit der Anwendung interner quantitativer Verfahren nur dann Bestand haben, wenn ein Vertrauensverhältnis zwischen beaufsichtigtem Institut und Aufsicht besteht. Für ein Abarbeiten von Kontrolllisten durch die Aufsicht ist die Thematik bei weitem zu komplex geworden.

6.4 Schlussfolgerungen für die zukünftige Gestaltung der Regulierung

Auf europäischer Ebene hat der Ausschuss der Weisen unter Bezug auf die Harmonisierung der Wertpapierabwicklung die Schwierigkeiten eines koordinierten Vorgehens bei gleichzeitiger Durchsetzung der Regulierung deutlich herausgearbeitet.[894] Diese Probleme sind auch bei der Regulierung des Zahlungsverkehrs in ähnlicher Form zu erkennen. Das Rautenmodell, und die im Vorkapitel beschriebene Alternative III der kaskadierenden Regulierung mit vertikalen Elementen, ermöglichen eine Erklärung und einen Lösungsansatz für diese Herausforderung.

In erster Linie sollte es im Zahlungsverkehr und verstärkt bei Sicherheitsfragen darum gehen, zu klären, wer diese Thematik zentral auf europäischer regulatorischer Ebene besetzt, und welches die Ansprechpartner auf nationaler Ebene sind. Erst wenn diese Fragen geklärt sind, können die Ziele, die mit entsprechenden Regulierungsinstrumenten verfolgt werden, definiert werden. Grundsätzlich zeichnet sich bei der vertikalen Regulierung, die von supranationaler Ebene geleistet wird, folgendes Spannungsfeld ab: Wird der „level playing field“-Argumentation gefolgt, werden die EU-Länder in der Zukunft kaum vermeiden können, supranationale Detailfragen zu bearbeiten und zu regulieren. Dies ist nicht nur aus Effiziengründen einleuchtend, da Doppelarbeiten vermieden und Kompetenzen bei entsprechender Kooperation gebündelt werden können. Der Gedanke einer gegenseitigen Anerkennung erfordert ein solches Vorgehen insbesondere bei sicherheitsrelevanten Fragestellungen. Theoretisch ist sonst eine Konstruktion denkbar, in der ein unsicherer Zahlungssystemanbieter eine Freigabe in Land A bekommt, und Land B, in dem er normalerweise keine Lizenz bekommen würde, gezwungen wäre, die Lizenz aus Land A anzuerkennen – europäisches Verordnungsrecht sticht nationales Recht. Wird argumentiert, es könnte bei nationalen Kompetenzzentren bleiben, ist Doppelarbeit unvermeidlich, da auf supranationaler Ebene der Vergleich der nationalen Regulierungen nötig würde.

[892] Fabritius (2001), S. 7.
[893] BIZ (2003d), S. 120 FN 88.
[894] Ausschuss der Weisen (2001).

Eine mögliche Alternative würde in der stringenten Verfolgung des kaskadierenden Pfades der Regulierung (Alternative I) bestehen. Auf supranationaler Ebene werden lediglich Grundsätze herausgearbeitet, die Umsetzung wird nationalen Behörden überlassen. Am Beispiel der digitalen Signatur lassen sich die Nachteile eines solchen Ansatzes jedoch aufzeigen. Durch die unterschiedliche Umsetzung der Richtlinie auf nationaler Ebene ist nunmehr das komplexe Problem der gegenseitigen Anerkennung und supranationalen Anwendung nationaler Signaturen entstanden. In der Folge wird signaturbasierten Produkten die Marktdurchdringung erschwert.

Zu der politischen Machtfrage, bei wem die Hoheit über Detailregelungen liegt, kommt die Frage nach den Personalressourcen. Statt auf EU-Ebene sämtliche Kompetenzen aufzubauen, wäre die Bildung nationaler Kompetenzzentren, die supranationale Aufgaben übernehmen können, unter beispielsweise der Leitung der EZB, ein möglicher alternativer Weg. Das US-amerikanische Federal Reserve System verfolgt im Kern einen solchen Ansatz, einzelne Federal Reserve Banken haben thematische Schwerpunkte, beispielsweise ist der Kartenzahlungsverkehr bei der Federal Reserve Bank of Philadelphia angesiedelt.

Die Idee, detaillierte Regelungen bereits auf EU-Ebene zu fixieren, ist aus Sicht des Autors unter einer Bedingung durchsetzbar. Handelt es sich im Zahlungsverkehr um neue Geschäftsfelder oder Technologien, die sukzessive von den Akteuren besetzt werden, ist es möglich supranational zu handeln. In diesem Fall sind kaum nationale Besonderheiten zu berücksichtigen, respektive der Markt kann sich an antizipierbare Regelungen anpassen, und dabei lokale Spezifika verarbeiten. In eine solche Kategorie des Vorgehens sind die EMSSO der EZB einzuordnen. Gleichwohl wird in der Folge der geplanten Weiterentwicklung der EMSSO zu klären sein, inwieweit die Ressourcen der EZB ausreichen, oder auf nationale Kompetenzen zurückgegriffen werden muss/sollte; zumal am Beispiel der formalen Methoden, die auf den Common Criteria basieren, und bei EMSSO Anwendung finden, offensichtlich wird, dass der Aufwand bei den nächsten Iterationen deutlich steigen wird.

Die potenzielle Stärke auf supranationaler Ebene formulierter Regularien lässt sich am Beispiel der Basel II Regelungen für Operationelle Risiken zeigen. Erst durch ein Vorgehen, dass bereits die Klassifikation dieser Risken zentral behandelt, wird es möglich a) eine notwendige kritische Masse an einheitlichen Daten zu erhalten und b) diese Daten so auszuwerten, dass in der Folge neue Regularien auf empirisch validierten Modellen aufbauen können. Im Bereich Operationeller Risiken hat die in den Vorkapiteln aufgeführte Entwicklung gezeigt, dass ohne regulatorischen Druck (zumindest nicht so „schnell“) das Risikomanagement auf Bankenseite ein erweitertes Blickfeld bekommen hätte. Einen Ansatz wie das vorgeschlagene Operational Risk Emergency and Analysis Centre in Kapitel 5.3.3.4 allein durch Kooperation von Wettbewerbern zu realisieren, ist schwer vorstellbar.

Zusammenfassend führen die verschiedene Trends im Zahlungsverkehr, die in den Vorkapiteln aufgezeigt wurden, zu einer Veränderung des regulatorischen und institutionellen Umfeldes mindestens in folgenden Punkten:

- Die verstärkte Notwendigkeit der Kooperation aller Regulierer wird erfolgreiche nationale Modelle zum Vorbild für europäische Institutionen werden lassen. Die Diskussion um einen europäischen ZKA, der sich momentan mit dem EPC zu formieren scheint, stützt diese These. Ebenso sollte zeitnah eine europäische Aufsichtsinstitution analog der BAFin etabliert werden, es sei denn, die EZB übernimmt deren Aufgaben einvernehmlich.

- Unklar ist zur Zeit, ob die Zusammenarbeit der Regulierer insbesondere auf europäischer Ebene über die existierende Vernetzung bei der gegenseitigen Teilnahme an Sitzungen hinreichend gewährleistet ist, oder ob paritätisch besetzte Gremien zu diesem Zweck gegründet werden sollten. Der beim BAFin angesiedelte Fachbeirat könnte ein Vorbild auch für europäische Regulierer sein.
- Bislang wird auf europäischer und auch internationaler Ebene (bei Basel II) das Konstrukt öffentlicher Konsultationen favorisiert, um insbesondere die Marktteilnehmer zur Stellungnahme zu bewegen. Allerdings bleibt hierbei zu berücksichtigen, dass ohne hinreichende Organisation des Marktes in entsprechenden Arbeitskreisen, Einzelstellungnahmen nur von etablierten großen Akteuren erwartet werden können, bedingt durch Ressourcenknappheiten kleiner und mittlerer Unternehmen. Genau diese sind aber zunehmend am Marktgeschehen beteiligt und sollten gerade im Hinblick auf ihre Innovationskraft berücksichtigt werden.
- Zur Zeit ist die Vielfalt im elektronischen Zahlungsverkehr einzelner EU-Länder durchaus gewollt. Nehmen zentralisierte Entscheidungen gemäß Alternative II im Vorkapitel mit vertikalen Regulierungspfaden mehr Raum ein, sollte politischer Konsens gefunden werden, inwieweit sich diese Tendenz mit dem Wunsch nach wettbewerblicher Vielfalt in Einklang bringen lässt. Solange die nationalen Institutionen mit der Sicherheit dieser Verfahren betraut sind, ist aus Sicht systemischer Risiken nicht zwingend ein Zustandswechsel erforderlich. Mit Voranschreiten der SEPA kann ohnehin ein Konzentrationsprozeß auf dem Markt für Zahlungsverkehrsdienstleistungen voranschreiten, der zur Zeit allerdings aufgrund kultureller Unterschiede im Bezahlverhalten der Marktteilnehmer schwierig zu prognostizieren ist.

7 Sicherer Elektronischer Zahlungsverkehr und Regulierung: Fazit und Ausblick

Der Zahlungsverkehr in Deutschland und Europa ist sowohl im Großbetrags-Zahlungsverkehr als auch bei den Individualzahlungen in den letzten Jahren angebotsseitig in starker Bewegung. Ein Haupttreiber dieser Entwicklung ist die gemeinsame europäische Währung, und der damit einhergehende Aufbau einer gemeinsamen Infrastruktur (SEPA). Während der europäische Bankensektor weitgehend national orientiert ist, und Übernahmen inländischer Banken durch ausländische Institute erst am Anfang stehen, findet der Wettbewerb der Zahlungssystementwickler und -anbieter zwischen Finanzinstituten und dritten Dienstleistern, insbesondere aus den Bereichen Informationstechnologie und Telekommunikation, statt. Der Zahlungsverkehrsmarkt ist ein sehr großer Markt: Ungefähr alle sechs Arbeitstage wird das gesamte Bruttosozialprodukt der EU-15-Länder einmal von dem größten Zahlungssystem der EU für Individualzahlungen TARGET bearbeitet.[895] Pro Tag werden über 200 Mio. Zahlungen im Massenzahlungsverkehr von verschiedenen Systemen in der EU verrechnet.[896]

Der Bankensektor wird in Deutschland und Europa als einer der am stärksten regulierten Wirtschaftsbereiche gesehen. Der Zahlungsverkehr gilt aufgrund seiner hohen volkswirtschaftlichen Bedeutung und der Gefahr systemischer Risiken als besonders schutz- und regulierungsbedürftig. So schwierig es ist, im Zahlungsverkehrsbereich öffentlich gewordene Schadensfälle zu finden, so deutlich wird an den in der Arbeit aufgezeigten Fällen, sofern es sich dabei um die vermutete sprichwörtliche Spitze des Eisbergs handelt, dass die Thematik „Sicherer Zahlungsverkehr“ von hoher volkswirtschaftlicher Bedeutung ist.

Es konnte in der vorliegenden Arbeit gezeigt werden, dass die Regulierung des Finanzsektors zwar fundamental durch das Anlegerschutzargument (aufgrund asymmetrischer Informationen und Machtasymmetrien) und das befürchtete Eintreten systemischer Schadensfälle begründet werden kann, es fehlt jedoch an weitergehenden Überlegungen, wie diese Regulierung institutionell und instrumentell ausgestattet werden kann und soll. In drei zentralen Kapiteln wurden:

a) die bislang nicht in dieser Form dokumentierten Regularien zu sicherheitsrelevanten Fragestellungen im elektronischen Zahlungsverkehr und die dazugehörigen Regulierer, sowohl private als auch staatliche, dargestellt (Kapitel 4/5),
b) die bestehenden und sich am Horizont abzeichnenden Risikomanagementverfahren für Operationelle Risiken abgehandelt und weitergehende Alternativen aufgezeigt (Kapitel 5) und
c) das Rautenmodell als Rahmen für die verschiedenen Fragestellungen der Regulierung (nicht nur) des Zahlungsverkehrs entwickelt und diskutiert (Kapitel 6).

Im Ergebnis lässt sich festhalten: Es gibt im Zahlungsverkehr sehr viele regulierende Institutionen und Instrumente, die von der internationalen Ebene bis zur betrieblichen reichen. Allerdings sind die Mehrzahl der Regelungen meist nicht mehr, als die formulierte Hoffnung des Regulierers, der Markt, respektive das Unternehmen, möge sich an ihnen orientieren. Am ausführlichsten geraten die Regulierungen im Großbetragszahlungsverkehr. Der Massenzahlungsverkehr gerät erst in jüngster Zeit vermehrt in den Fokus der Regulierer, vor allem der Aufsicht, der Zentralbanken und der EU-Kommission. Gerade der Massenzahlungsverkehr ist nahe am Endverbraucher, technische Innovationen, unter anderem beim mobilen Bezahlen,

[895] Berechnet aus SVR (2003), Tabelle 3*, S. 501 und EZB (2003c), S. 6 und EZB (2003e), S. 4.
[896] EZB (2002d), S. 19.

finden in rascher Folge statt, und es gilt, das notwendige Vertrauen der Konsumenten in die Bezahlsysteme zu erhalten. Eine Möglichkeit besteht in der Suche nach wirksamen regulatorischen Vorgaben. Grundlage für eine solche Suche sollte Datenmaterial über die wirksamen Risiken im Bankensektor allgemein und im Zahlungsverkehr im Besonderen sein.

Auf Seiten der Banken und Sparkassen wurde mit der Aufnahme und Betonung Operationeller Risiken in die Verhandlungen zur Neuen Basler Eigenkapitalvereinbarung ein wichtiger erster Schritt zur quantitativen Erfassung dieser Risiken getan. Der politische Prozess, der zu einer Verabschiedung der Basel II Vereinbarung führen soll, ist ins Stocken geraten, der Zeitplan zur Umsetzung der dort beschlossenen Maßnahmen mehrfach verschoben worden. Gleichwohl hat bereits in der Konsultationsphase eine tiefgreifende Auseinandersetzung der Finanzbranche und der Regulierer mit Operationellen Risiken begonnen. In Kapitel 5 wird der Ansatz zur Erfassung Operationeller Risiken ausführlich erörtert, und die sich darum lagernden Risikomanagementprozesse beleuchtet. In der Arbeit wird aufgezeigt, dass diese Maßnahmen sämtlich in die richtige risikobegrenzende Richtung gehen, und gerade im Zahlungsverkehr Wirkung zeigen können. Allerdings nur für den Fall, dass Basel II nicht zum zahnlosen Papiertiger verkommt, der auf angesammelten und lediglich rudimentär ausgewerteten Daten sitzt. Der Vorschlag eines weiterführenden Ausbaus sowohl der Datensammlung mit ergänzenden Parametern als auch eines gemeinsam mit der Aufsicht betriebenen Auswertungszentrums für Operationelle Risiken geht davon aus, eine Win-Win-Situation für die Finanzinstitute und die Aufsichtsorgane/Regulierer zu realisieren. Die Aufsicht selbst ist zur Erkenntnis gelangt, dass externe quantitative Vorgaben durch die Regulierer (Basel I), bedingt durch die zunehmende Komplexität der Bank- und Finanzdienstleistungen und darunterliegenden Prozesse, an ihre Grenzen gestoßen sind. Der Aufsichts-Trend geht zu qualitativen Vorgaben (u. a. best practices) und internen quantitativen Modellen, deren Güte von der Aufsicht überprüft werden soll. Im vorgestellten Modellansatz wird es der Aufsicht möglich, kooperativ mit dem Markt die Feinschrauben der in Basel II verwendeten Modelle zu justieren, und ein Gefühl für die marktseitige Relevanz der Vorgaben zu bekommen. Auf Marktseite ist ein wesentlicher Vorteil dieses Vorgehens, dass die breitere Datenbasis ein besseres Risikomanagement mit entsprechendem Einsparungspotenzial ermöglicht.

Der aktuelle Aktionsplan für Finanzdienstleistungen der EU zeigt, dass auf europäischer Ebene die Notwendigkeit zur Veränderung erkannt ist, die Umsetzung dieser Erkenntnis lässt allerdings bislang noch zu wünschen übrig. Es besteht jedoch zum gegenwärtigen Zeitpunkt allgemeiner Umstrukturierungen die Chance, institutionell neue Verhaltensmuster einzuüben, da beispielsweise noch kein europäisches Aufsichtsamt existiert, und auch das EPC als potenzielles europäisches ZKA gerade erst gegründet wurde. Die Verhandlungsmuster und -strukturen gilt es nunmehr auf Grundlage klar definierter Ziele und Kompetenzen zu entwickeln.

Das in Kapitel 6 entwickelte Rautenmodell liefert einen Analyserahmen für die Regulierung des Zahlungsverkehrs und verdeutlicht das Spannungsfeld, in dem sich die Regulierer bewegen. Der vorgenommene Abgleich des Modells mit der Wirklichkeit zeigt die notwendigen Handlungsfelder der Regulierer auf. Anhand der möglichen Gestaltungsparameter der Regulierung und ihrer Instrumente (u. a. hoheitlich versus Selbstregulierung oder Ko-Regulierung, „security by obscurity“ versus „security by transparency“ und quantitativ versus qualitativ) wurde als wesentlicher Punkt herausgearbeitet, dass die Zielbestimmung im Zahlungsverkehr nicht das Problem darstellt. Vielmehr muss die Machtfülle und Kompetenz einzelner Institutionen sowohl in horizontaler als auch in vertikaler Richtung erst eindeutig geklärt werden, bevor die Instrumente zur Diskussion stehen. Dies wird unter anderem bei der Analyse des von der EU-Kommission eingebrachten Konsultationspapiers für einen neuen

einheitlichen Rechtsrahmen im europäischen Zahlungsverkehr deutlich. Dort wechseln sich Abschnitte, die lediglich Umrisse skizzieren, mit der Diskussion von Detailfragen ab.

Zur Klärung anstehender Regulierungsfragen müsste ein zentrales Kompetenzzentrum, beispielsweise die EZB, die Koordination des weiteren Vorgehens leiten; an dieser Stelle stoßen öffentliche Konsultationen an sichtbare Grenzen. Neben der Bestimmung von Kompetenzzentren auf nationaler wie supranationaler Ebene ist ferner die Frage der Koordination der jeweiligen Institutionen institutionell und organisatorisch zu klären. Bei einem kaskadierenden Regulierungspfad können die Regelungen entlang der Bezugsebene (supranational bis lokal) verfeinert werden – und treffen meist auf etablierte Strukturen. Kommen vertikale Elemente der Regulierung ins Spiel, ist dies nicht so deutlich der Fall. Ein solches (vertikales) Vorgehen muss allen Akteuren verständlich kommuniziert werden, sonst wird spätestens die nationale aufsichtliche Überprüfung der Vorgaben schwierig. Im Sinne eines „level playing field"-Ansatzes sind vertikale Ansätze nicht nur in sicherheitsrelevanten Gebieten der Bezahlverfahren, sondern gerade bei Bezahlinnovationen wie beispielsweise elektronischem Geld zu begrüßen.

Kooperation der Aufsicht und der Marktteilnehmer bei einer gleichzeitigen Umorientierung aufsichtlicher Strukturen auf qualitative Ansätze und quantitative interne Modelle bedeutet nun nicht ein Verschmelzen von Aufsichts- und Marktinteressen. Es wird im Zeitverlauf der Einübung neuer Verhaltensmuster immer wieder erhebliche Schwierigkeiten bei der Umsetzung der neuen Muster geben. Es bleibt abzuwarten, in welcher Höhe sich Effizienzgewinne realisieren lassen, die unter anderem aus den im Rahmen dieser Arbeit aufgezeigten Risikomanagementansätzen für den Umgang mit Operationellen Risiken (im elektronischen Zahlungsverkehr) resultieren.

Sind die untersuchten Zahlungssysteme nicht zuletzt aufgrund der aufsichtlichen Anforderungen sicher genug? Die Antwort lautet deutlich und bestimmt: Es kommt auf die Perspektive an. Im Großzahlungsverkehr zeichnen sich nicht nur in Europa zunehmend hohe Sicherheitsstandards ab. Im Massenzahlungsverkehr ist die Lage differenzierter, da nicht zuletzt aufgrund der um ein Vielfaches höheren Transaktionszahlen und der wesentlich höheren Zahl an Akteuren (Konsumenten, Händler, Dienstleister etc.) Sicherheit schwieriger zu gewährleisten ist. Aus Sicht der Konsumenten wurde bei der Gestaltung der rechtlichen Rahmenbedingungen viel bewegt, der Haftungsausschluss für Schadensfälle ist (fast) umfassend. Die Händler und die Anbieter der Zahlungssystemdienstleistungen allerdings haben noch einen steinigen Weg vor sich, bevor Operationellen Risiken, und dabei insbesondere kriminellen Aktivitäten, ein wirkungsvoller Riegel vorgeschoben werden kann.

In der vorliegenden Arbeit wurde das Trapezmodell aus einer Detailanalyse eines spezifischen Marktsegments abgeleitet, des Marktes für elektronischen Zahlungsverkehr. Dieser wurde wiederum unter dem Blickwinkel der Sicherheit untersucht. Die Ergebnisse im Hinblick auf die institutionelle Gestaltung regulatorischer Aufgaben, sowohl im hoheitlichen Sinne als auch im selbstregulatorischen Umfeld, erscheinen tragfähig für eine mögliche Ausweitung der Fragestellung, beispielsweise im Hinblick auf die regulatorische Gestaltung des gesamten Finanzsektors oder anderer Wirtschaftssektoren. Die Harmonisierung des EU-Binnenmarktes wird in dieser Richtung noch manch eine Frage aufwerfen.

Literaturverzeichnis

Bei Angabe von Internetadressen (URL) ist der Tag des letzten Abrufs des Dokuments in Klammern eingefügt.

Akerlof (1970): Akerlof, G. (1970): The Market for Lemons: Quality Uncertainty and the Market Mechanism, Quarterly Journal of Economics, 89, S. 488-500

AKSIS (2003): AKSIS – Ziele, Organisation, Programm, www.aksis.de/AKSIS_inhalt.htm (13.08.2003)

Anders (2001): Anders, U. (2001): Qualitative Anforderungen an das Management operativer Risiken, in: Die Bank, 6/2001, S. 442-446

Andersen (2002): Andersen Financial Services Industry (Hrsg.) (2002): Herausforderung Basel II, 2. erweiterte Auflage, Eschborn/Frankfurt a. M., 4/2002

Anderson (2001): Anderson, R. (2001): Security Engineering – A Guide to Building Dependable Distributed Systems, Wiley Computer Publishing, New York

Anderson (2003): Anderson, R. (2003): Diners Club (SA) Pty Ltd v Anil and Vanita Singh, Brief an Master Turner, Royal Courts of Justice, London, 19.02.2003

Arnfield (2000): Arnfield, B. und Arnfield R. (2000): E-Payments Security – Challenges and Opportunities for Banks in the B2C Market, 5/2000, Lafferty Publications, Dublin, Irland

Arounopoulos (2002): Arounopoulos, S. und Kaufmann, M. (2002): Die Zukunft der GeldKarte – Neue Einsatzfelder für die Chipkarte der deutschen Kreditwirtschaft, in: Ketterer (2002), S. 232-249

Artopoeus (1998): Artopoeus, W. (1998): Kreditrisiko – Erfahrungen und Ansichten eines Aufsehers, Vortrag beim Symposium „Kreditrisiko“ der Deutschen Bundesbank, 24.11.1998, Frankfurt a. M.

Ausschuss der Weisen (2001): Schlussbericht des Ausschusses der Weisen über die Regulierung der europäischen Wertpapiermärkte, 15.2.2001, Brüssel

BAFin (2002a): Vereinbarung über die Zusammenarbeit der Bundesanstalt für Finanzdienstleistungsaufsicht und der Deutschen Bundesbank bei der Beaufsichtigung der Kredit- und Finanzdienstleistungsinstitute, 31.10.2002, Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn

BAFin (2002b): Veröffentlichung der Endfassung des Rundschreibens über „Mindestanforderungen an das Kreditgeschäft der Kreditinstitute“, 20.12.2002, Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn

BAFin (2002c): Mindestanforderungen an das Kreditgeschäft der Kreditinstitute, Rundschreiben 34/2002, 20.12.2002, Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn

BAKred (1995): BAKred (1995): Verlautbarung über Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute, 23.10.1995, Bundesaufsichtsamt für das Kreditwesen, Bonn

BAKred (1998): Erläuterungen zu einzelnen Regelungen der Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute, 08.04.1998, Bundesaufsichtsamt für das Kreditwesen, Bonn

BAKred (2000a): Jahresbericht 2000, Bundesaufsichtsamt für das Kreditwesen, Bonn

BAKred (2000b): Mindestanforderungen an die Ausgestaltung der Internen Revision der Kreditinstitute, Rundschreiben 1/2000, 17.01.2000, Bundesaufsichtsamt für das Kreditwesen, Bonn

BAKred (2001): Ergänzende Hinweise zu den Mindestanforderungen an das Betreiben von Handelsgeschäften der Kreditinstitute Revisionsberichte und Marktgerechtigkeitsprüfung, 21.09.2001, Bundesaufsichtsamt für das Kreditwesen, Bonn

Baldwin (1999): Baldwin, R. und Cave, M. (1999): Understanding Regulation – Theory, Strategy, and Practice, Oxford University Press, Oxford

Bartsch (2003): Bartsch, C. (2003): Was kommt nach SET? 3D-Secure, SPA/UCAF, www.zahlungsverkehrsfragen.de/spa_ucaf_3dfsecure.html (09.09.2003)

Barvell (2002): Barvell, K. (2002): Risks and Developments in Payment Systems, IMF, Washington, 28.08.2002

Bauer (2003): Bauer, V. (2003): Potenziale des Angebots von Bonitätsprüfungen und Zahlungsgarantien in Banken – Analyse am Beispiel der LBBW im Bereich ePayment, Diplomarbeit am Institut für Wirtschaftspolitik und Wirtschaftsforschung, Universität Karlsruhe (TH)

BdB (2003a): Umsätze im bargeldlosen Zahlungsverkehr, www.bdb.de/html/statistikservice/stat_banken.asp?channel=164710&cm=0#zahlungsverkehr, (05.06.2003)

BdB (2003b): Der europäische Zahlungsverkehr im Wandel – Daten, Fakten, Argumente, 06/2003, Bundesverband deutscher Banken, Berlin

Beau (2002): Beau, D. und Martin, C. (2002): Security of Payment Systems on the Internet, in Banque de France Monthly Bulletin Nr. 101, 05/2002

Beeck (2000): Beeck, H. und Kaiser, T. (2000): Quantifizierung von Operational Risk mit Value-at-Risk, in: Johanning (2000), S. 633-653

Belcher (2002): Belcher, T. und Yoran, E. (2002): Riptech Internet Security Threat Report – Attack Trends for Q3 and Q4 2001, Riptech Inc., Alexandria

Berentsen (1997): Berentsen, A. (1997): Supervision and Regulation of Network Banks, firstmonday, Vol. 2, Nr. 8, 4.8.1997, www.firstmonday.dk/issues/issue2_8

Bielefeld (2003): Bielefeld, F. (2003): Traditionelle Kennzahlen der Banksteuerung – Möglichkeiten und Grenzen, Vortrag vor dem Arbeitskreis „Strategieentwicklung und Controlling in Banken“, Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., 28.03.2003, Hamburg

Birch (2001): Birch, D. (2001): Retail Electronic Money – A medium-term perspective, in: proceedings of Digital Transactions Forum, 10/2001, APSCA, Hong Kong

BIZ (1990): Report of the Committee on Interbank Netting Schemes of the Central Banks of the Group of Ten countries, 11/1990, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1994): Risk Management Guidelines for Derivatives, Basel Committee on Banking Supervision, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1995): Risk Management for Electronic Banking and Electronic Money, Committee on Payment and Settlement Systems, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1996): Security of Electronic Money, Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, 8/1996, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1997):Core Principles for Effective Banking Supervision, Basle Committee on Banking Supervision, 9/1997, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1998a):Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision, 3/1998, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1998b): Managing Change in Payment Systems, Policy Papers Nr. 4, Monetary and Economic Department, 5/1998, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1998c): Operational Risk Management, Risk Management Sub-group of the Basle Committee on Banking Supervision, 9/1998, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1998d): Framework for Internal Control Systems of Banking Organisations, Basle Committee on Banking Supervision, 9/1998, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1998e): Enhancing Bank Transparency, Transparency Sub-group of the Basle Committee on Banking Supervision, 9/1998, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1999a): Retail Payments in Selected Countries: A Comparative Study, Committee on Payment and Settlement Systems, 8/1999, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (1999b): Enhancing Corporate Governance for Banking Organisations, Basle Committee on Banking Supervision, 9/1999, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2000): Statistics on Payment Systems in the Group of Ten Countries, Committee on Payment and Settlement Systems, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2000a): The Contribution of Payment Systems to Financial Stability, Commitee on Payment and Settlement Systems, Papers presented at a workshop on payment systems at CEMLA, Mexiko City, 5/2000, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2000b): Clearing and Settlement Arrangements for Retail Payments in Selected Countries, Committee on Payment and Settlement Systems, 9/2000, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2000c): Summary of Initiatives – Electronic Banking Group of the Basel Committee for Banking Supervision, 10/2000, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001a): Pillar 2 (Supervisory Review Process), Supporting Document to the New Basel Capital Accord, Consultative Document, Basel Committee on Banking Supervision, 1/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001b): Grundprinzipien für Zahlungsverkehrssysteme, die für die Stabilität des Finanzsystems bedeutsam sind – Bericht der Task Force für Grundsätze und Praktiken in Zahlungsverkehrssystemen, Ausschuss für Zahlungsverkehrs- und Abrechnungssysteme, 1/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001b engl.): Core Principles for Systemically Important Payment Systems, Commitee on Payment and Settlement Systems, 1/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001c): Consultative Document, Operational Risk, Supporting Document to the New Basel Capital Accord, Basel Committee on Banking Supervision, 1/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001d): Consultative Document. The New Basel Capital Accord, Basel Committee on Banking Supervision, 1/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001e): Konsultationspapier, Überblick über die Neue Basler Eigenkapitalvereinbarung, Basler Ausschuss für Bankenaufsicht, 1/2001, Bank für Internationalen Zahlungsausgleich, Übersetzung der Deutschen Bundesbank, Frankfurt a. M.

BIZ (2001f): The implications of electronic trading in financial markets, Committee on the Global Financial System, 1/2001, Bank für Internationalen Zahlungsausgleich

BIZ (2001g): Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, 5/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001h): Internal Audit in Banks and the Supervisor's Relationship with Auditors, Basel Committee on Banking Supervision, 8/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001i): Working Paper on the Regulatory Treatment of Operational Risk, Basel Committee on Banking Supervision, 9/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001j): Electronic finance: a new perspective and challenges, Monetary and Economic Department, BIS Papers Nr. 7, 11/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001k): Results of the Second Quantitative Impact Study, Basel Committee on Banking Supervision, 05.11.2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001l): Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, 12/2001, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2001m): Background Information Committee on Payment and Settlement Systems, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002):The Relationship between Banking Supervisors and Banks' External Auditors, Basel Committee on Banking Supervision, 01/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002a): The Quantitative Impact Study for Opertional Risk: Overview of Individual Loss Data and Lessons Learned, Basel Committee on Banking Supervision, 01/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002b): Operational Risk Data Collection Exercise – 2002, Basel Committee on Banking Supervision, 04.06.2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002c): Results of Quantitative Impact Study 2.5, Basel Committee on Banking Supervision, 25.06.2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002d): Basel Committee reaches agreement on New Capital Accord issues, Bank für Internationale Zahlungsausgleich, Pressemitteilung vom 10.7.2002

BIZ (2002e): Sound Practices for the Management and Supervision of Operational Risk, 7/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002f): Internal Audit in Banks and the Supervisor's Relationship with Auditors: A Survey, Basle Committee on Banking Supervision, 8/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002g): Policy issues for central banks in retail payments, Report of the Working Group on Retail Payment Systemes, Konsultationspapier, 9/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002h): Profil, 10/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002i): Quantitative Impact Study 3 – Instructions, Basel Committee on Banking Supervision, 10/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002j): Quantative Impact Study 3 – Technical Guidance, Basel Committee on Banking Supervision, 10/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2002k): Overview Paper for the Impact Study, Basel Committee on Banking Supervision, 10/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003a): Sound Practices for the Management and Supervision of Operational Risk, 02/2003, Basel Committee on Banking Supervision, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003b): Policy issues for central banks in retail payments, 3/2002, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003c): Überblick über die Neue Basler Eigenkapitalvereinbarung, Konsultationspapier, Basler Ausschuss für Bankenaufsicht, 04/2003, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003d): The New Basel Capital Accord, Basler Ausschuss für Bankenaufsicht, 04/2003, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003e): The Basel Committee on Banking Supervision, Basler Ausschuss für Bankenaufsicht, Basel, www.bis.org/bcbs/aboutbcbs.htm (30.06.03)

BIZ (2003f): The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected, Basel Committee on Banking Supervision, Risk Management Group, 03/2003, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003g): Quantitative Impact Study 3 – Overview of Global Results, Basler Ausschuss für Bankenaufsicht, 05.05.2003, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003h): Supplementary Information on QIS3, Basler Ausschuss für Bankenaufsicht, 27.05.2003, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003i): Management and Supervision of Cross-Border Electronic Banking Activities, Basler Ausschuss für Bankenaufsicht, 07/2003, Bank für Internationalen Zahlungsausgleich, Basel

BIZ (2003j): Risk Management Principles for Electronic Banking, Basler Ausschuss für Bankenaufsicht, 07/2003, Bank für Internationalen Zahlungsausgleich, Basel

BMÖLS (1998): IT-Sicherheitshandbuch für die öffentliche Verwaltung, Teil 1: IT-Sicherheitsmanagement, Bundesministerium für öffentliche Leistung und Sport. Version 1.0, 10/1998

Board (2002): Board of Governors of the Federal Reserve System; Office of the Comptroller of the Currency und Securities and Exchange Commission (2002): Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 30.08.2002

Böhle (1998): Böhle, K. und Riehm, U. (1998): Blütenträume – Über Zahlungssysteminnovationen und Internet-Handel in Deutschland, Wissenschaftliche Berichte, FZKA 6161, 12/1998, Institut für Technikfolgenabschätzung und Systemanalyse, Forschungszentrum Karlsruhe Technik und Umwelt

Böhle (2000): Böhle, K., Krueger, M. u.a. (2000): Electronic Payment Systems – Strategic and Technical Issues, Background Paper No. 1, Electronic Payment Systems Observatory, Sevilla, Spanien

Böhle (2002): Böhle, K. (2002): Internet-Zahlungssysteme in der Europäischen Union, in: Ketterer (2002), S. 45-61

Böhle (2002a): Böhle, K. (2002a): Integration von Payment Systemen – Bindung mit Hindernissen, in: Electronic Commerce InfoNet, www.ecin.de/zahlungssysteme/integration/ (06.06.2003)

Bond (2003): Bond, M. und Zielinski, P. (2003): Decimalisation table attacks for PIN cracking, Technical Report, Nr. 560, Computer Laboratory, University of Cambridge

Bonn (1998): Bonn, J. (1998): Bankenkrisen und Bankenregulierung, Gabler, Wiesbaden

Borkovec (2000): Borkovec, M. und Klüppelberg, C. (2000): Extremwerttheorie für Finanzzeitreihen – ein unverzichtbares Werkzeug im Risikomanagement, in: Johanning (2000), S. 219-244

Bräuhäuser (2002): Bräuhäuser, M.; Biltzinger, P., Lorenz, C. (2002): Qualitative Risikoanalyse – Methodische Vorgehensweise in der IT-Beratungspraxis, in Rossbach (2002), S. 55-69

Brink van den (2002): Brink van den, J. (2002): Operational Risk Management, Vortragsunterlagen, CFSforum – Operational Risk, 21.02.2002

Bröhl (2000): Bröhl, A.-P., Bröschel, W. (Hrsg.) (2000): Das V-Modell, Verlag Oldenbourg

BSI (1999a): Information security management – Part 1: Code of practice for information security management, British Standard BS 7799-1:1999, Bundesamt für Sicherheit in der Informationstechnik, Bonn

BSI (1999b): Information security management – Part 2: Specification for information security management systems, British Standard BS 7799-2:1999, Bundesamt für Sicherheit in der Informationstechnik, Bonn

BSI (2000): IT-Grundschutzhandbuch – Standard-Sicherheitsmaßnahmen, Version 01/2000, Bundesamt für Sicherheit in der Informationstechnik

Buchmann (1999): FlexiPKI – Realisierung einer flexiblen Public-Key-Infrastruktur, Technical Report Nr. TI-22/99, Technische Universität Darmstadt

Buhr (2000): Buhr, R. (2000): Risikomanagement – Messung von Betriebsrisiken – ein methodischer Ansatz, in: Bank – Zeitschrift für Bankpolitik und Bankpraxis, Nr. 3, S. 202-207

Burghof (1996): Burghof, H.-P. und Rudolph, B. (1996):Bankenaufsicht: Theorie und Praxis der Regulierung, Gabler, Wiesbaden

Büschgen (1998): Büschgen, H. (1998): Bankbetriebslehre – Bankgeschäfte und Bankmanagement, 5. Aufl., Gabler, Wiesbaden

Chakam et al. (2002): Chakam, A.; Heitmann, A.; Leibold, K.; Stölzle, R.; Stroborn, K. (2002): Internet-Zahlungssysteme aus Sicht der Verbraucher – IZV5, Institut für Wirtschaftspolitik und Wirtschaftsforschung, Universität Karlsruhe (TH)

Cheswick (1994): Cheswick, W.R. und Bellovin, S.M. (1994): Firewalls and Internet Security – Repelling the Wily Hacker, Addison Wesley, AT&T. Zitiert in: Palensky et al. (2000), S. 31

Committee on Banking and Financial Services (2000): The Future of Electronic Payments: Roadblocks and Emerging Practices, Expertenanhörung vor dem Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy, U.S. House of Representatives, 19.09.2000, Washington DC, http://commdocs.house.gov/committees/bank/hba66988.000/hba66988_0.HTM (07.11.2002)

CYTEX (2001): Cyber Terror Exercise – CYTEX: Angriff von kritischen Infrastrukturen, IABG, Ottobrunn, 12.-14.11.2001

Dennig (2002): Dennig, U. (2002): Noch Ineffizienzen im Auslands-Zahlungsverkehr!, in: Wirtschaftsdienst 2/2002, HWWA-Forum, S. 107-111

Deutsche Bundesbank (1998): Elektronische Öffnung der Deutschen Bundesbank – Externe Spezifikationen, Version 4.1, CD-ROM, 1998, Frankfurt a. M.

Deutsche Bundesbank (1999): Gesetz über das Kreditwesen, Bankrechtliche Regelungen 2, 3/1999, Frankfurt a. M.

Deutsche Bundesbank (2000a): RTGS^{plus} – Das neue Individual-Zahlungssystem der Deutschen Bundesbank, Monatsbericht 06/2000, S. 61-73, Frankfurt a. M.

Deutsche Bundesbank (2000b): Electronic Banking aus bankenaufsichtsrechtlicher Perspektive, Monatsbericht 12/2000, S. 43-59, Frankfurt a. M.

Deutsche Bundesbank (2001a): Zahlungsverkehr und Wertpapierabwicklung in Deutschland im Umfeld europäischer und internationaler Entwicklungen, Symposium am 05.09.2001 in Frankfurt a. M., Tagungsunterlagen, Deutsche Bundesbank, Frankfurt a. M.

Deutsche Bundesbank (2001b): RTGS^{plus} – Das Echtzeit-Bruttosystem für den Euro mit liquiditätssparenden Elementen, Stand 7/2001, Frankfurt a. M.

Deutsche Bundesbank (2002a): RTGS^{plus} – erfolgreich am Markt etabliert, Monatsbericht 04/2002, Deutsche Bundesbank, Frankfurt a. M.

Deutsche Bundesbank (2002a): Elektronischer Massenzahlungsverkehr (EMZ) – Das moderne Massenzahlungssystem der Deutschen Bundesbank, 3. überarbeitete Aufl., Stand 7/2002, Frankfurt a. M.

Deutsche Bundesbank (2002a): Stellungnahme der Deutschen Bundesbank zu dem Arbeitsdokument „Ein möglicher Rechtsrahmen für einen einheitlichen Zahlungsverkehrsraum im Binnenmarkt“, 31.07.2002, Frankfurt a. M.

Deutsche Bundesbank (2002c): Aktuelle Entwicklungen im unbaren Zahlungsverkehr der Deutschen Bundesbank – Informationsveranstaltung für Kreditinstitute im Dezember 2002, 12/2002, Frankfurt a. M.

Deutsche Bundesbank (200d): RTGS^{plus} – Ein Jahr nach Betriebsaufnahme, Deutsche Bundesbank, Frankfurt a. M.

Deutsche Bundesbank (2003a): Statistiken zum Zahlungsverkehr in Deutschland 1997-2001, Stand Februar 2003, Frankfurt a. M.

Deutsche Bundesbank (2003b): Neue Mindestanforderungen an das Kreditgeschäft: MaK und Basel II, Monatsbericht 01/2003, S. 45-58, Frankfurt a. M.

Deutsche Bundesbank (2003c): Bankenstatistik März 2003, Statistisches Beiheft zum Monatsbericht 1, Frankfurt a. M.

Deutsche Bundesbank (2003d): Neue bankaufsichtliche Mindestanforderungen für Kreditinstitute – Drittes Basler Konsultationspapier, MaK und Wege zur Umsetzung, Expertenkonferenz, 03.06.2003, Tagungsunterlagen, Frankfurt a. M.

Deutsche Bundesbank (2003e): Dienstleistungsangebot der Deutschen Bundesbank im bargeldlosen Zahlungsverkehr, http://www.bundesbank.de/zv/zv_dienstleistungen.php (10.08.2003)

Dewatripont (1994): Dewatripont, M. und Tirole, J. (1994): The Prudential Regulation of Banks, 2. Auflage 1999, MIT Press, Cambridge, Massachusetts

Dickertmann (1996): Dickertmann, D. und Feucht, R. (Hrsg.) (1996): Der Kreditkartenmarkt in Deutschland: eine ökonomische Analyse, Fachbuchreihe des Informationsdienstes Source, Neuwied

Dorn (1997a): Dorn, J. A. (Hrsg.) (1997): The Future of Money in the Information Age, Cato Institute, Washington D.C.

Dorn (1997b): Dorn, J. A. (1997): Introduction – The Future of Money, in: Dorn (1997a), S. 1-12

Duwendag et al. (1999): Duwendag, D., Ketterer, K.-H., Kösters, W., Pohl, R., Simmert, D. B., Geldtheorie und Geldpolitik in Europa, Springer, Berlin u.a., 5. Aufl.

EBA (2002): STEP2 – Pan-European Bulk Payment Processing System: Functional Overview, 10.10.2002, Euro Banking Association

EBA (2003): STEP1 – Information note, Euro Banking Association, 07/2003

ECBS (2003): Annual Report 2002, European Committee for Banking Standards, Brüssel

Eller et al. (2002): Eller, R.; Gruber, W.; Reif, M. (Hrsg.) (2002): Handbuch Operationelle Risiken, Schäffer-Poeschel Verlag, Stuttgart

Enroth (2001): Enroth, G. (2001): Cashing in, in: Finance on Windows, Autumn 2001, S. 64-65

EPC (2002): Euroland: Our Single Payment Area!, White Paper Summary, European Payments Council, 05/2002

EPS (2003): Kartengestützter Zahlungsverkehr: Stand und Entwicklungstendenzen, EURO Payment Solutions GmbH, Vortrag, 15.05.2003, München

Escher (1999): Escher, M. (1999): Aktuelle Rechtsfragen des Zahlungsverkehrs im Internet, Internet: www.gassner.de/escher/zvi-txt.html (22.01.01)

EU (2001): Rahmenbeschluss des Rates vom 28.05.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln, 28.05.2001, Brüssel

EU (2002): Komitologie, www.europarl.eu.int/trans._de/Abc/k/Komitologie.htm (29.08.2002)

EU (2003): Konferenz und Studie der Kommission geben Aufschluss über Sicherheit und öffentliche Wahrnehmung des elektronischen Zahlungsverkehrs, EU Institutions Press Releases IP/03/1265, 18.09.2003, Brüssel

EuroHandelsinstitut (2002): Kartengestützte Zahlungssysteme im Einzelhandel, Ergebnis der Jahresuntersuchung 2002 – Fakten, Analysen, Hintergründe aus der empirischen Forschung des EuroHandelsinstituts, Verlag EHI – EuroHandelsinstitut GmbH, Köln

Europäische Gemeinschaften (2000a): Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt der Europäischen Gemeinschaften, 19.01.2000, Brüssel

Europäische Gemeinschaften (2000b): Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"): Amtsblatt der Europäischen Gemeinschaften, 17.07.2000, Brüssel

Europäische Gemeinschaften (2000c): Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, Amtsblatt der Europäischen Gemeinschaften, 27.10.2000, Brüssel

Europäische Gemeinschaften (2001): Verordnung 2560/2001des Europäischen Parlaments und des Rates vom 19. Dezember 2001 über grenzüberschreitende Zahlungen in Euro, Amtsblatt der Europäischen Gemeinschaften, 28.12.2001, Brüssel

EZB (1998a): Bericht über elektronisches Geld, 8/1998, Europäische Zentralbank, Frankfurt a. M.

EZB (1998b): Third Progress Report on the TARGET Projekt, 11/1998, Europäische Zentralbank, Frankfurt a. M.

EZB (1999): Meinung der EZB zur Directive 1 und 2 zu „prudential supervision of the business of electronic money institution", Europäische Zentralbank, Frankfurt a. M.

EZB (1999a): Der institutionelle Rahmen des Europäischen Systems der Zentralbanken, Monatsbericht, 7/1999, S. 59-67, Europäische Zentralbank, Frankfurt a. M.

EZB (1999b): The Effect of Technology on the EU Banking Systems, 7/1999, Europäische Zentralbank, Frankfurt a. M.

EZB (1999c): Improving cross-border retail payment services – The Eurosystems' View, 9/1999, Europäische Zentralbank, Frankfurt a. M.

EZB (1999d): Cross-border payments in TARGET – A users' survey, 11/1999, Europäische Zentralbank, Frankfurt a. M.

EZB (2000a): Die Europäische Zentralbank, 4/2000, Europäische Zentralbank, Frankfurt a. M.

EZB (2000b): Role of the Eurosystem in the field of payment systems oversight, 6/2000, Europäische Zentralbank, Frankfurt a. M.

EZB (2000c): TARGET update 2000, 8/2000, Europäische Zentralbank, Frankfurt a. M.

EZB (2000d): Fragen rund um den Einsatz von Elektronischem Geld, Monatsbericht 11/2000, S. 56-68, Europäische Zentralbank, Frankfurt a. M.

EZB (2000e): TARGET-Leitfaden für Kreditinstitute, Europäische Zentralbank und Deutsche Bundesbank, Version 3.0, 11/2000, Europäische Zentralbank, Frankfurt a. M.

EZB (2001): Leitlinie der Europäischen Zentralbank über ein transeuropäisches automatisches Echtzeit-Brutto-Express-Zahlungsverrechnungssystem (Target), EZB/2001/3, 26.04.2001, Frankfurt a. M.

EZB (2001a): Payment and securities settlement systems in the European Union (Blue Book), 3. Auflage, 06/2001, Europäische Zentralbank, Frankfurt a. M.

EZB (2001b): Towards an integrated infrastructure for credit transfers in Euro, 11/2001, Europäische Zentralbank, Frankfurt a. M.

EZB (2002): Leitlinie der Europäischen Zentralbank zur Änderung der Leitlinie EZB/2001/3 über ein transeuropäisches automatisches Echtzeit-Brutto-Express-Zahlungsverrechnungssystem (TARGET), EZB/2002/1, 27.02.2002, Frankfurt a. M.

EZB (2002a): Electronic Money System Security Objectives (EMSSO)– According to the common criteria methodology, 3/2002, Europäische Zentralbank, Frankfurt a. M.

EZB (2002b): The role of the Eurosystem in payment and clearing systems, Monatsbericht der Europäischen Zentralbank, 4/2002, Europäische Zentralbank, Frankfurt a. M., S. 47-59

EZB (2002c): Aufsichtsstandards für Euro-Massenzahlungssysteme, 08.07.2002, Europäische Zentralbank, Frankfurt a. M.

EZB (2002d): Blue Book, Payment and securities settlement systems in the European Union, Addendum incorporating 2000 figures, 7/2002, Europäische Zentralbank, Frankfurt a. M.

EZB (2002e): E-payments in Europe – the Eurosystem's perspective, Issues Paper, 16.9.2002, Europäischen Zentralbank, Frankfurt a. M.

EZB (2002f): The long-term evolution of TARGET, ECB Press Release, 24.10.2002, Europäische Zentralbank, Frankfurt a. M.

EZB (2002g): Öffentliches Konsultationsverfahren – TARGET2: Grundsätze und Struktur, 16.12.2002, Europäische Zentralbank, Frankfurt a. M.

EZB (2003a): Elektronisierung des Zahlungsverkehrs in Europa, in: Monatsbericht Mai 2003, Europäische Zentralbank, Frankfurt a. M., S. 65-78

EZB (2003b): Electronic Money System Security Objectives – According to the Common Criteria Methodology, 5/2003, Europäische Zentralbank, Frankfurt a. M.

EZB (2003c): TARGET – Annual Report 2002, 04/2003, Europäische Zentralbank, Frankfurt a. M

EZB (2003d): Standards für die Überwachung von Euro-Massenzahlungssystemen, 06/2003, Europäische Zentralbank, Frankfurt a. M.

EZB (2003e): Brief Overview over TARGET, 11.08.2003, Europäische Zentralbank, Frankfurt a. M.

Fabritius (2001): Fabritius, H. G. (2001): Zahlungsverkehrspolitik der Deutschen Bundesbank, in Deutsche Bundesbank (2001a)

Fabritius (2003a): Fabritius, H. G. (2003): The evolving role of central banks in payment systems: service providers and/or overseers?, 12-13.06.2003, CPSS Global Conference on Payment Systems, Frankfurt a. M.

Fabritius (2003b): Die Rolle der Zentralbanken im Zahlungsverkehr – Ansichtssache, in: Börsen-Zeitung, 29.08.2003, S. 8

Fama (1980): Fama, E. (1980): Banking in the Theory of Finance, in: Journal of Monetary Economics, Vol. 6, S. 39-57

Federal Reserve System (2002): The Future of Retail Electronic Payments Systems: Industry Interviews and Analysis, Board of Governaors of the Federal Reserve System Staff Study, Nr. 175, Federal Reserve Staff for the Payments System Development Committee, Federal Reserve System, 12/2002

FinDAG (2002): Gesetz über die Bundesanstalt für Finanzdienstleistungsaufsicht, 22.04.2002, BGBl. I S. 1310-1315, Bonn

Firstgate (2003): Informationen, Begriffe und Tipps – Firstgate click & buy™, Firstgate Internet AG, Köln

Fluhr (2003): Fluhr, M. (Hrsg.) (2003): OMNICARD-Newsletter, 06/2003, www.omnicard.de (10.06.2003)

Fontaine (2003): Fontaine, J. (2003): Debitkarten im Internet, Die Bank – Zeitschrift für Bankpolitik und Bankpraxis, April 2003

Frey (2003): Frey, T. (2003): Top 10 Inventions in Money Technology – Last Century's Big Money-Related Innovations, The DaVinci Institute, Louisville, USA, 04.08.2003

Friederich (1998a): Friederich, H.-J. (1998a): Euro-Zahlungsverkehr: Die neue Clearing-Infrastruktur ab 1999, Präsentationsfolien zum Vortrag im Rahmen der European Banking Technology Fair '98 in Frankfurt a. M. am 03.11.1998

Friederich (1998b): Friederich, H.-J. (1998b): Organisatorische Vorbereitungen der Zentralbanken auf den Euro-Zahlungsverkehr, in Stein, J. H. von: Handbuch EURO, Verlag C.H. Beck, München 1998

Friederich (1999): Friederich, H.-J. (1999): Convergence of gross and net systems – the EAF/ELS example, Presentation at SIBOS Munich, 9/1999

Friederich (2000): Friederich, H.-J. (2000): Interbank clearing in the euro-zone, Vortrag anläßlich der SWIFT Regionalkonferenz in Zentral- und Osteuropa in Prag, Tschechische Republik, 24.3.2000

Friederich (2001): Friederich, H.-J. (2001): Weiterentwicklung im Dienstleistungsangebot der Deutschen Bundesbank, in Deutsche Bundesbank (2001a)

Fullarton (1845): Fullarton, J. (1845): On the Regulation of Currencies in: O´Brien, Denis (Hrsg.) (1994):The Foundations of Monetary Economics, 6 Volumes, Vol. 5, Pickering & Chatto Publishers, London

Gartner Group (2001): On-line fraud prevention, White Paper for the E-Commerce fraud prevention network, 14.03.2001

Geisinger (2001): Geisinger, M. und Buchberger, R. (2001): State-of-the-Art-Report – Das Treuhand-Bezahlverfahren der S-ITT, in: BIT, Nr. 4/2001, S. 30

Geyer-Schulz et al. (2003): Geyer Schulz, A.; Heitmann, A.; Neumann, A.; Stroborn, K. (2003): Strategic Positioning Options for Scientific Libraries in Markets of Scientific and Technical Information – The Economic Impact of Digitalization, in: Jounal of Digital Information, Vol. 4, Band 2, http://jodi.ecs.soton.ac.uk/Articles/v04/i02/Geyer-Schulz/ (05.06.2003)

Goodhart (2000): Goodhart, C.A.E. (2000): Can Central Banking Survive the IT Revolution?, in: International Finance, Vol. 3, S. 189-209

Handelsblatt (2002): Internet-Banking hat Sicherheitsschwächen, Internetfakten, 27.08.2002

Hartmann (1998): Hartmann, We. (1998): Speech at Sibos Helsinki, Closing Plenary Session on 24.09.1998, BIS Review 84/1998

Hartmann (1999): Hartmann, Wu. (1999): Das neue Überweisungsgesetz, in: Die Bank, Nr. 8/1999, S. 536-541

Hartmann (2000): Hartmann, M. (2000): Elektronisches Geld und Geldpolitik – Eine Analyse der Wechselwirkungen, Wiesbaden

Hartmann (2003): Hartmann, M. und Stroborn, K. (2003): Zahlungsverkehrspolitik – die Gestaltungsmacht der Regulierer, in: Kotz, H.; Simmert, D.; Hofer, M. (erscheint voraussichtlich Ende 2003): Wirtschafts- und Geldpolitik in gesellschaftlicher Verantwortung, Festschrift zum 60. Geburtstag von Prof. Dr. Karl-Heinz Ketterer, Duncker & Humblot, Berlin

Heise (2001): Bankenaufsicht plant Sicherheitschecks bei Internet-Banken, heise online news, 18.01.01, www.heise.de/newsticker/data/ae-18.01.01-000/

Heise (2002a): Website versuchte PayPal-Passwörter abzufangen, heise online news, 25.04.2002, www.heise.de/newsticker/data/hod-25.04.02-001/ (25.04.2002)

Heise (2003a): Ermittlungen wegen geklauter Kreditkartendaten, heise online news, 20.02.2003, www.heise.de/newsticker/data/jk-20.02.03-005/ (20.02.2003)

Heise (2003b): Musik und Spiele stehen bei zahlenden Internet-Nutzern hoch im Kurs, heise online news, 27.05.2003, www.heise.de/newsticker/data/jk-27.05.03-000/ (06.06.2003)

Heise (2003c): Mastercard plant Handy-Überweisungen von Kreditkarte zu Kreditkarte, heise online news, 24.06.2003, www.heise.de/newsticker/data/hod-24.06.03-000/ (24.06.2003)

Heitmann (2002): Heitmann, A. (2002): Rechtliche Rahmenbedingungen des Bezahlens im Internet: EU-Recht und deutsche Gesetzgebung, in: Ketterer (2002), S. 275-293

Hennig (2002): Hennig, K. (2002): Strategieentwicklung für ein Dienstleistungsunternehmen in der Digital Economy am Beispiel von Bertelsmann Financial Services, Diplomarbeit am Institut für Wirtschaftspolitik und Wirtschaftsforschung, Universität Karlsruhe (TH)

Hofmann (2002a): Hofmann, G. (Hrsg.) (2002): Basel II und MaK – Vorgaben, bankinterne Verfahren, Bewertungen, Bankakademie Verlag, Frankfurt a. M.

Hofmann (2002b): Hofmann, M. (2002): Identifizierung, Quantifizierung und Steuerung operationeller Risiken in Kreditinstituten, Bankakademie Verlag, Frankfurt a. M.

Hruby (2002): Hruby, A. (2002): Public Key Infrastrukturen, Diplomarbeit am Institut für Wirtschaftspolitik und Wirtschaftsforschung, Universität Karlsruhe (TH)

Hutter (2002): Hutter, R. (2002): Wie lassen sich offene und hochtechnologisierte Gesellschaften schützen – das Beispiel Cyber Terror, Task Force Zukunft der Sicherheit der Bertelsmann Stiftung, Gutachten für die Bertelsmann Stiftung, Berlin

HVB (2001): Trend-Book 2001, HypoVereinsbank, München

Iclear (2003): Allgemeine Geschäftsbedingungen der EuroCoin iclear GmbH, Stand 01.03.2003

IDW EPS 523 (2003): Entwurf IDW Prüfungsstandard: Prüfung der Funktionsfähigkeit der Internen Revision bei Kreditinstituten, Stand 10.02.2003, in: Die Wirtschaftsprüfung - Der Berater der Wirtschaft, Düsseldorf, Nr. 6/2003, S. 286 ff.

IDW ERS FAIT 2 (2002): Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce, Stand 20.08.2002, in: Die Wirtschaftsprüfung - Der Berater der Wirtschaft, Düsseldorf, Nr. 16/2002, S. 878 ff.

IDW PS 260 (2001): Das interne Kontrollsystem im Rahmen der Abschlussprüfung, Stand 27.08.2001, in: Die Wirtschaftsprüfung - Der Berater der Wirtschaft, Düsseldorf, Nr. 16/2001, S. 821 ff.

IDW PS 321 (2002): Interne Revision und Abschlussprüfung, Stand 04.06.2002, in: Die Wirtschaftsprüfung - Der Berater der Wirtschaft, Düsseldorf, Nr. 13/2002, S. 686 ff.

IDW PS 330 (2002): Abschlußprüfung bei Einsatz von Informationstechnologie, Stand 24.09.2002, in: Die Wirtschaftsprüfung - Der Berater der Wirtschaft, Düsseldorf, Nr. 21/2002, S. 1167 ff.

IDW PS 720 (2000): Fragenkatalog zur Prüfung der Ordnungsmäßigkeit der Geschäftsführung und der wirtschaftlichen Verhältnisse, Stand 13.09.2000, in: Die Wirtschaftsprüfung - Der Berater der Wirtschaft, Düsseldorf, Nr. 7/2000, S. 326 ff.

IDW RS FAIT 1 (2002): IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce, Stand 24.09.2002, in: Die Wirtschaftsprüfung - Der Berater der Wirtschaft, Düsseldorf, Nr. 21/2002, S. 1157 ff.

IMF (2000a): Financial System Soundness – A Factsheet, 30.03.2000, IMF, Washington, www.imf.org/external/np/exr/facts/banking.htm (09.09.2003)

IMF (2000b): Financial Sector Assessment Program (FSAP) A Review: Lessons from the Pilot and Issues Going Forward, 27.09.2000, IMF, Washington,

IMF (2003a): Articles of Agreement of the International Monetary Fund, IMF, Washington

IMF (2003b): IMF Surveillance– A Factsheet, 04/2003, IMF, Washington, www.imf.org/external/np/exr/facts/surv.htm (09.09.2003)

IMF (2003c): How the IMF Promotes Global Economic Stability – A Factsheet, 09/2003, IMF, Washington, www.imf.org/external/np/exr/facts/globstab.htm (19.09.2003)

IMFTWB (2002): Financial Sector Assessment Program – Experience with the Assessment of Systemically Important Payment Systems, approved by Stefan Ingves and Cesare Calari, 19.04.2002, International Monetary Fund – The World Bank, Washington

Initiative D21 (2002): Initiative D21 (2002) (Hrsg.): Arbeitsgruppe 5 – Sicherheit und Vertrauen im Internet, Projekt: „CERT Infrastruktur Deutschland“, Berlin, 24.04.2002

Interexa (2002): ORC-Operational Risk Center – Gesamtlösung zur Steuerung operationaler Risiken nach den Vorschlägen des Basler Ausschusses für Bankenaufsicht (Basel II), Produktbeschreibung, Version 2.1, interexa internet solutions, Mainz

IntFinDAG (2002): Gesetz über die integrierte Finanzdienstleistungsaufsicht, 22.04.2002, BGBl. I. S. 1310-1337, Bonn

ISO (2003): Introduction, 15.04.2003, International Organization for Standardization, Genf, www.iso.org/iso/en/aboutiso/introduction/index.html (09.09.2003)

ISO/IEC TR 13335-1:1998 (1998): Information technology – Security techniques – Guidelines for the management fo IT Security, Teil 1: Concepts and Models for IT Security, International Organization for Standardization, Genf

ISO/IEC TR 13335-2:1998 (1998): Information technology – Security techniques – Guidelines for the management fo IT Security, Teil 2: Managing and Planning IT Security, International Organization for Standardization, Genf

ISO/IEC TR 13335-3:1998 (1998): Information technology – Security techniques – Guidelines for the management fo IT Security, Teil 3: Techniques for the management of IT Security, International Organization for Standardization,Genf

ISO/IEC TR 13335-4: 2000 (2000): Information technology – Security techniques – Guidelines for the management fo IT Security, Teil 4: Selection of safeguards, International Organization for Standardization, Genf

ISO/IEC TR 13335-5: 2000 (2000): Information technology – Guidelines for the management fo IT Security, Teil 5: Safeguards for external Connections, International Organization for Standardization, Genf

ISO 15408-1(1999): ISO/IEC 15408 – 1:1999 (1999):Common Criteria for Information Technology Security Evaluation, Part 1, International Organization for Standardization, Genf

ISO 15408-2(1999): ISO/IEC 15408 – 2:1999 (1999):Common Criteria for Information Technology Security Evaluation, Part 2, International Organization for Standardization, Genf

ISO 15408-3(1999): ISO/IEC 15408 – 3:1999 (1999):Common Criteria for Information Technology Security Evaluation, Part 3, International Organization for Standardization, Genf

Jameson (1998): Jameson, R. (1998): Getting the Measure of the Beast, in: Risk, Nr. 11, 1998, S. 38-41

Johanning (2000): Johanning L. und Rudolph, B. (Hrsg.) (2000): Handbuch Risikomanagement, Band 1: Risikomanagement für Markt-, Kredit- und operative Risiken, Uhlenbruch Verlag, Bad Soden/Ts.

Johnson et al. (1998): Johnson, O. E.G. mit Abrams, R. K. et al. (1998): Payment Systems, Monetary Policy, an the Role of the Central Bank, International Monetary Fund, Washington

Jörg (2002): Jörg, M. und Roßbach, P. (2002): Messung und Bewertung Operationeller Risiken, in: Rossbach (2002), S. 71-93

Kern (2002): Kern, S. (2002): Die EU auf steinigem Weg zum Finanzbinnenmarkt, Aktuelle Themen – EU-Finanzmarkt Spezial, Nr. 231, 04.06.2002, Deutsche Bank Research, Frankfurt a. M.

Kern (2003): Kern, S. (2003): Reform der EU-Regulierungs- und Aufsichtsstrukturen: Zwischenbericht, EU-Monitor – Finanzmarkt Spezial, Nr. 4, 19.08.2003, Deutsche Bank Research, Frankfurt a. M.

Ketterer (2002): Ketterer, K.-H. und Stroborn, K. (Hrsg.) (2002): Handbuch ePayment: Zahlungsverkehr im Internet; Systeme, Trends und Perspektiven, Mit einem Vorwort von Bundesbankpräsident Ernst Welteke, Deutscher Wirtschaftsdienst, Köln

Ketterer (2003): Ketterer, K.-H. und Ohmeyer, E. (2003): Die Transaktionsbank – ein neuer Banktyp entsteht, in: Karlsruher Transfer, Nr. 29, Verein Karlsruher Wirtschaftsingenieure, Karlsruhe (erscheint 1. Quartal 2004)

Klein (1997): Klein, S. (1997): Hürdenlauf electronic cash, Die Entstehung eines elektronischen kartengestützten Zahlungssystems als sozialer Prozess, Mölln

Kok (2002): Kok, Low Siang (2002): Singapore Electronic Legal Tender (SELT)- A Proposed Concept, in OECD (2002), The Future of Money, Paris, S. 147-158

KOM (1998): Kommission der Europäischen Gemeinschaften (1998): Finanzdi€nstleistungen: Abstecken eines Aktionsrahmens, Mitteilung der Kommission, KOM(1998)625, 28.10.1998, Brüssel

KOM (1999): Kommission der Europäischen Gemeinschaften (1999): Finanzdi€nstleistungen: Umsetzung des Finanzmarktrahmens: Aktionsplan, Mitteilung der Kommission, KOM(1999)232, 11.05.1999, Brüssel

KOM (2000a): Kommission der Europäischen Gemeinschaften (2000a): Mitteilung der Kommission an den Rat und das Europäische Parlament, Massenzahlungsverkehr im Binnenmarkt, KOM(2000)36, S. 4 ff., Brüssel

KOM (2000b): Kommission der Europäischen Gemeinschaften (2000b): Institutional Arrangements for the Regulation and Supervision of the Financial Sector, Internal Market Directorate General, 01/2000, Brüssel

KOM (2001): Kommission der Europäischen Gemeinschaften (2001): Mitteilung der Kommission an den Rat, das Europäische Parlament, die Europäische Zentralbank, den Wirtschafts- und Sozialausschuss und Europol zur Vorbeugung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln, KOM(2001)0011, Brüssel

KOM (2002): Kommission der Europäischen Gemeinschaften (2002): Regulation on cross-border payments in euros to apply from 1 July 2002 – frequently asked questions, EU Institutional press release, 27.06.2002, Brüssel

KOM (2003a): Kommission der Europäischen Gemeinschaften (2003a): FSAP-Folgemaßnahmen – Überprüfung des Integrationsstands der EU-Finanzmärkte, Insurance Committee, MARKT/2532/03-DE, 13.11.2003, Brüssel

KOM (2003b): Kommission der Europäischen Gemeinschaften (2003b): Ein neuer Rechtsrahmen für den Zahlungsverkehr im Binnenmarkt, Mitteilung der Kommission an den Rat und das Europäische Parlament, Konsultationspapier, KOM(2003)718, 02.12.2003, Brüssel

KPMG (1998): Integriertes Risikomanagement, Broschüre, 7/1998, Berlin

KPMG (2000): Reformen im Zeichen von Internationalität, Transparenz und Kontrolle, Broschüre, 12/1998, Berlin

KRITIS (1999): Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland, Kurzbericht der Ressortarbeitsgruppe KRITIS, Entwurfsversion 7.95, 12/1999

Krüger (2001): Krüger, Malte (2001): Innovation and Regulation – The Case of E-Money Regulation in the EU, Background Paper No. 5, Electronic Payment Systems Observatory

Krüger (2002): Krüger, Malte (2002): Die Bedeutung von mobilen Zahlungsformen, in: Ketterer (2002), S. 363-373

Kupiec (2001): Kupiec, Paul (2001): The New Basel Capital Accord: The Devil is in the (Calibration) Details, Monetary and Exchange Affairs Departement, IMF Working Paper WP 01/113, 8/2001, Washington

Kupitz (1983): Kupitz, R. (1983): Die Kreditwirtschaft als wettbewerbspolitischer Ausnahmebereich, Harri Deutsch, Frankfurt a. M.

Lang (2000): Lang, F.-J. (2000): Risk Management, Secunet Security Networks AG, Eschborn

Langenbucher (2001): Langenbucher, K. (2001): Die Risikozuordnung im bargeldlosen Zahlungsverkehr, Münchner Universitätsschriften, Reihe der Juristischen Fakultät, Bd. 160, Verlag C.H. Beck, München

Leibold (2003): Leibold, K. und Stroborn, K. (2003): Internet-Zahlungssysteme aus Sicht der Verbraucher – IZV6, Institut für Wirtschaftspolitik und Wirtschaftsforschung, Universität Karlsruhe (TH)

Lelieveldt (2001): Lelieveldt, S. (2001): Research study on the integration of e-payments into the online transaction process, Study commissioned by the Institute for Prospective Technological Studies as a part of the ePayments Systems Observatory Project, 12/2001, Sevilla, Spanien

Loscocco et al. (1999): Loscocco, P.; Smalley, S.; Muckelbauer, P.; Taylor, R.; Turner, J.; Farrell, J. (1999): The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments, National Security Agency, USA

LZB (1999): EAF – das Euro-Clearing-System in Frankfurt a. M. (Broschüre), 9/1999, Landeszentralbank in Hessen, Frankfurt a. M.

Mander (2003): Mander, B. (2003): Basel Bunkum, in: Newsmakers – Central Bankers in the news, 09.06.2003, S. 2, www.centralbanking.co.uk/newsmakers/index.htm (10.06.2003)

Markus (1999): Markus, M. (1999): Marktüberblick: Karten im Handel, in: Card Forum 05/1999, S. 26

MasterCard (2003): MasterCard SecureCodeTM – Merchant Implementation Guide, 03/2003, MasterCard International

McDonough (1998): McDonough, W. (1998): Managing change in payment systems, in: BIZ (1998b), S. 9-17

Medosch (2001): Medosch, A. und Röttgers, J. (Hrsg.)(2001): Netzpiraten – Die Kultur des elektronischen Verbrechens, Heise Verlag, Hannover

Meister (2000): Meister, E.; Vollbracht, R.; Baum, J. (2000): Internationale bankaufsichtliche Eigenkapitalstandards für Kreditinstitute, in: Johanning (2000), S. 755-773

Moneybookers (2003a): Factsheet, www.moneybookers.com/factsheet.html (23.06.2003)

Moneybookers (2003b): Allgemeine Geschäftsbedingungen, www.moneybookers.com /app/help.pl?s=terms (09.09.2003)

Morasch (2002): Morasch, K. (2002): Wettbewerbspolitik und Regulierung, Skriptum, Universität der Bundeswehr, München

Müller (1979): Müller, J. und Vogelsang, I. (1979): Staatliche Regulierung, Nomos, Baden-Baden

Müller (1997): Müller, G. und Pfitzmann, A. (Hrsg.) (1997): Mehrseitige Sicherheit in der Kommunikationstechnik – Verfahren, Komponenten, Integration, Bd. 1. Addison-Wesley-Longman, Bonn, Reading, Massachusetts u.a.

Müller (1998): Müller, G. und Stapf, K.-H.(Hrsg.) (1998): Mehrseitige Sicherheit in der Kommunikationstechnik – Erwartung, Akzeptanz, Nutzung, Bd. 2. Addison-Wesley-Longman, Bonn, Reading, Massachusetts u.a.

Müller (1999): Müller, G. und Rannenberg, K. (Hrsg.) (1999): Multilateral Security in Communications, Bd. 3, Technology, Infrastructure, Economy, Addison-Wesley-Longman, München, Reading, Massachusetts u.a.

Münch (2002): Münch, I. (Hrsg.) (2002): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft, Bundesamt für Sicherheit in der Informationstechnik

Neugebauer (2002): Neugebauer, A. (2002): Divergierende Fallentscheidungen von Wettbewerbsbehörden – Institutionelle Hintergründe, Arbeitspapiere Nr. 26, Institut für Genossenschaftswesen, Westfälische Wilhelms-Universität Münster

Niemann (2001): Niemann, N. (2001): Organisatorische Sicherheit im IT-Sicherheitsmanagement – Elektronische Zahlungsmethoden im Spannungsfeld internationaler Richtlinien, Diplomarbeit am Institut für Wirtschaftspolitik und Wirtschaftsforschung, Universität Karlsruhe (TH)

Nitschke (2002): Nitschke, R. und Weiß, J. (2002): PayPal – The new world currency?, www.novosec.com (09.09.2003)

NWIR (2002): Anmerkung zu BGH, Urteil vom 16.04.2002 – CI ZR 375/00, Forum Neues Wirtschaftsrecht, www.nwir.de/aktuell/kreditkarteAnmerkung.pdf (05.06.2003)

o.V. (2001): Noch Sicherheitslücken im E-Banking – Bankenaufsicht erarbeitet Sicherheitscheck für Banken und Finanzinstitute, 1/2001, Frankfurter Allgemeine Zeitung, Frankfurt a. M.

o.V. (2002a): Nokia, Nordea and Visa International to pilot the world's first Electronic Mobile Payment Services based on dual chip technology, Pressemitteilung Nordea, 09/2002, www.nordea.com/eng/press/release/20010924.asp?navi=press (05.06.2003)

o.V. (2002b): Kreditkarten von morgen denken mit – Dank Chip werden Kreditkarten immer intelligenter, Direkt – Informationen für die Partner der Euro Kartensysteme, Eurokartensysteme, Ausgabe 1, 05/2002, Frankfurt a. M.

o.V. (2003): Quick und der Euro – eine Erfolgsstory, www.quick.at/html/news/Kurzartikel.pdf, (25.01.2003)

o.V. (2003a): T-Online erwirbt Bundesligarechte, 10.04.2003, www.ecin.de/news/2003/04/10/05655/ (06.06.2003)

o.V. (2003b): Die Abzocke der falschen Treuhänder, Spiegel Online, 24.07.2003, www.spiegel.de/netzwelt/politik/0,1518,258310,00.html (24.07.2003)

o.V. (2003c): CC product evaluation picks up steam, NetworkWorldFusion, www.nwfusion.com/news/2003/0804commoncriteria.html?page=2 (04.08.2003)

o.V. (2003d): EU intervention takes SEPA a step closer, in: Electronic Payments International, Juli 2003

o.V. (2003e): Banks respond to new EC regulation, in: Financial Sector Technology, Juli/August 2003

o.V. (2003f): Exklusiv bei L'TUR: Postbank-Kunden können Reisepreis sofort online überweisen, fun communications, www.fun.de, Karlsruhe

o.V. (2003g): Visa Kartenzahlungen 2002 weiter auf dem Vormarsch, Pressemitteilung, 27.03.2003, Frankfurt a. M.

o.V. (2003h): MasterCard's VPN: Banknet – An Overview, http://www.mastercardintl.com/docs/vpn_fact_sheet.pdf (09.09.2003).

O'Brian (2000): O'Brian, T. und Murray, B. (2000): E-Payments – Emerging Strategies for Value Exchange in eCommerce – a Lafferty Report, Lafferty Publications Ltd., Dublin

OECD (2002a): Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security, OECD, Paris

OECD (2002b): The Future of Money, OECD, Paris

Ovink (2002): Ovink, B. (2002):VISA – Security in E.Commerce, European Financial Management & Marketing Konferenz, e-Security – Security & Virtual Financial Services, Tagungsunterlagen, 26.11.2002, Paris

Palensky et al. (2000): : Palensky, Peter; Sauter, Thilo; Schwaiger,Christian (2000): Security und Feldbusse – ein Widerspruch?, it + ti – Informationstechnik und Technische Informatik 42, 4, S. 31

Peter (2000): Peter, A., Vogt, H.-J. und Kraß, V. (2000): Management operationeller Risiken bei Finanzdienstleistern, in: Johanning (2000), S. 655-677

Plate (1997): Plate, A. (1997): IT-Sicherheitsmanagement in der internationalen Standardisierung, URL: www.bsi.bund.de/literat/tagungsb/plate.htm (20.06.2001)

Pluto (2003): Pluto, K. (2003): MaK und Mindestanforderungen an bankinterne Ratingsysteme – ein Vergleich, in: Deutsche Bundesbank (2003d)

Porter (1990): Porter, M. (1990): Wettbewerbsstrategien: Methoden zur Analyse von Branchen und Konkurrenten, Frankfurt a. M.

Porter (1992): Porter, M. (1992): Wettbewerbsvorteile, 3. Aufl., Campus, Frankfurt, New York

Power (2002): Power, R. (2002): 2002 CSI/FBI Computer Crime and Security Survey, Vol. VIII, Nr. 1, Frühjahr 2002, Computer Security Institute

Preuß (2002): Preuß, W. (2002): Kredit- und Debitkarten: Stand und Entwicklung der Kartenkriminalität, in: Fluhr, M. (2002): Neue und bewährte Applikationsfelder der Chipkarte, Kongressdokumentation OMNICARD 2002, 16.-18.10.2002, Berlin, S. 239-243

Raepple (1998): Raepple, M. (1998): Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, dpunkt-Verlag, Heidelberg

Rehm (2001): Rehm, H. (2001): Veränderungen im Zahlungsverkehr des Kreditgewerbes – neue Produkte und Techniken, in: Deutsche Bundesbank (2001a)

Reis (2000): Reis, K.-H. und Stockmeier, W. (2000): Die Rolle der EDV-Revision im IT-Sicherheitsprozess, in: KES Zeitschrift für Kommunikations- und EDV-Sicherheit, Nr. 6, 12/2000, S. 34f.

Riedl (2002): Riedl, G. (2002): Der bankbetriebliche Zahlungsverkehr – Infrastruktur-Innovationen und Wandel der Zahlungsverkehrsabwicklung, Physica-Verlag, Heidelberg

Riehm (1998): Riehm, U. (1998): Sammelbesprechung: Elektronische Zahlungssysteme in der sozialwissenschaftlichen Technikforschung, in: TA-Datenbanknachrichten, Nr. 2, 7. Jhg., Juni 1998, erscheint online: www.itas.fzk.de/deu/tadn/tadn298/rieh298a.htm (05.06.2003)

Röhm (2000): Röhm, A. W. (2000): Sicherheit offener Elektronischer Märkte: Modellbildung und Realisierungskonzept, Lohmar, Köln

Roßbach (2002): Roßbach, P. und Locarek-Junge, H. (Hrsg.) (2002): IT-Sicherheitsmanagement in Banken, Bankakademie Verlag, Frankfurt a. M.

Rudolph (2000): Rudolph, B. (2000): Entwicklungslinien im Risikomanagement, in: Johanning (2000), S. 15-52

Sahajwala (2000): Sahajwala, R. und Van den Bergh, P. (2000): Supervisory Risk Assessment And Early Warning Systems, Basle Committee on Banking Supervision, Working Papers, Nr. 4, 12/2000, Bank für Internationalen Zahlungsausgleich, Basel

Saitz (1998): Saitz, B. und Braun, F. (Hrsg.)(1998): Das Kontroll- und Transparenzgesetz: Herausforderungen und Chancen für das Risikomanagement, Gabler, Wiesbaden

Santos (2000): Santos, J. (2000): Bank capital regulation in contemporary banking theory: a review of the literature, BIS Working Papers, Nr. 90, Bank für Internationalen Zahlungsausgleich, Basel

Schilder (2001): Schilder, A. (2001): Banking in the new economy: a supervisory perspective, BIS Review 16/2001, S. 1-3

Schlueter (1997): Schlueter, C. und Shaw, M. (1997): A Strategic Framework for Developing Electronic Commerce, in: IEEE Internet Computing, Vol. 1, Nr. 6, Nov./Dez. 1997, S. 20-28

Schmidt (2001): Schmidt, R. (2001): Der Allfinanzaufsicht fehlt die europäische Dimension, in: Finanzplatz, Nr. 2, Oktober 2001, S. 6-8

Schmidt (2003): Schmidt, J. (2003): Verschlüsselung als Bärendienst, heise Security, 05.09.2003, www.heise.de/security/artikel/print/40073 (09.09.2003)

Schneier (2000): Schneier, B. (2000): Secrets and lies – Digital Security in a Networked World, Wiley Computer Publishing, New York

Schneier (2003): Schneier, B. (2003): The Risks of Cyberterrorism, in: Crypto-Gram, Counterpane Internet Security, 15.06.2003, www.counterpane.com/crypto-gram.html

Schürer (2002): Schürer, T. (2002): Die Kreditkarte im Internet, in: Ketterer (2002), S. 206-231

Secunet (2001): Rechtliche Besonderheiten im E-Banking/E-Commerce, Unterlagen zur Tagung der IHK Frankfurt, 21.2.2001, Frankfurt a. M.

Seifert (1984): Seifert, E. (1984): Privilegierung und Regulierung im Bankenwesen, Nomos, Baden-Baden

Siegert (2002): Siegert, J. (2002): Digitales Geld, Vortrag auf Trierer Symposium Digitales Geld, 20.6.2002, Trier

Sienkiewicz (2002): Sienkiewicz, S. und Bochicchio, M. (2002): The Future of E-Commerce Payments, Conference Summary 19.06.2002, Federal Reserve Bank of Philadelphia

Simon (2002): Simon, W. (2002): Systematische Identifikation, Erfassung und Bewertung Operationeller Risiken, in: Eller (2002), S. 125-152

SIZ (2000): Schutzprofil SIZ-PP – Schutzprofil Sicherheit für IT-Gesamtsysteme der Finanzdienstleister, Sparkassen Informatik Zentrum, Version 2.0, 02/2000, SIZ, Bonn

Smart-e(2002): EMV-Chip für Kredit- & Debitkarten: sicher bezahlen im Internet, Whitepaper, Security Research & Consulting GmbH, Bonn

Spencer (2001): Spencer, P. (2001): Regulation of the payments market and the prospect for digital money, in: BIZ (2001c), S. 69-79

Stapf (1998): Stapf, K.-H. (1998): Psychologische Betrachtungen zum Sicherheitsbegriff, in: Müller (1998), S. 45-68

Stark (2001): Stark, J. (2001): Zahlungsverkehr und Wertpapierabwicklung in Deutschland im Umfeld europäischer und internationaler Entwicklungen, Begrüßungsansprache, in: Deutsche Bundesbank (2001a)

Stickelmann (2002): Stickelmann, K. (2002): Operationelles Risiko – Abgrenzung, Definition und Anforderungen nach Basel II, in: Eller (2002), S. 3-42

Stigler (1971): Stigler, G. (1971): The Theory of Economic Regulation, 2 Bell J. of Econ. 3. – The Optimum Enforcement of Laws (1970), 78 J. Pol. Econ. 526

Stocker et al. (2001): Stocker, G.; Naumann, M.; Buhr, R.; Kind, R.; Schwertl, M. (2001): Qualitatives und quantitatives Controlling und Management von Operational Risk, in: Zeitschrift für das Kreditwesen, 12/2001, S. 677-687

Stögbauer (2002): Stögbauer, Ch. (2002): Miss es oder vergiss es! Quantitative Operational-Risk-Modellierung, in: Eller (2002), S. 179-204

Stroborn (2000): Stroborn, K. (2000): Zahlungsmittel im Internet – eine Übersicht, in: Töpper, A., Müller, P. (Hrsg.) (2000): Stiftung Warentest: Qualitätskennzeichnung beim E-Commerce, Abschlussbericht: Anhang, S. 1-13

SVR (2001): Für Stetigkeit – gegen Aktionismus, Jahresgutachten 2001/02, Sachverständigenrat zur Begutachtung der gesamtwirtschaft-lichen Entwicklung, 14.11.2001, Wiesbaden

SVR (2003): Staatsfinanzen konsolidieren – Steuersystem reformieren, Jahresgutachten 2003/04, Sachverständigenrat zur Begutachtung der gesamtwirtschaftlichen Entwicklung, 12.11.2003, Wiesbaden

SWIFT (2002): Sibos 2002 – Contesting the level playing field?, Sibos issues onsite, Brüssel, 4.10.2002

SWIFT (2003a): Annual Report 2002, SWIFT SRCL, La Hulpe, Belgien

SWIFT (2003b): SWIFTNet FIN – Planning Guide for the Multi-vendor SIPN Environment, Version 3.0, 02/2003, SWIFT, Belgien

TelekomForum (2003): Kick-Off – Veranstaltung – FocusGruppe e-payment, 12.06.2003, TelekomForum e.V., Köln

Terres (2001): Terres, P. (2001): Basel II: Die geplante Baseler Eigenkapitalübereinkunft schadet den Sparkassen und dem Finanzplatz in Deutschland, Volkswirtschaft Spezial, DGZ DekaBank, Abteilung Volkswirtschaft + Information, 16.01.2001

Thies (2002): Thies, K., DG Bank AG (2002): Praktisches IT-Risk-Management, 5. Euroforum Kongress am 19.9.2001, Tagungsunterlagen

Thodén (1999): Thodén, N. (1999): Managing the Vulnerability of Banks to Information Technology Related Criminal Type Risks, Dissertation Nr. 2206, Universität St. Gallen

Tichy (1990): Tichy, G. (1990): Bankengröße und Effizienz, in Kredit und Kapital, 23.Jgh., S. 358-388

Traufetter (2003): Traufetter, G. (2003): Schatzkarte für Terroristen, Der Spiegel, 32/2003, 04.08.2003, www.spiegel.de/spiegel/0,1518,259739,00.html (6.8.2003)

Ullrich (2001): Ullrich, T. (2001): Zahlungsverkehr – ein Kerngeschäft der Banken, in: Deutsche Bundesbank (2001a)

Visa (2003): **3-D Secure**™ System Overview, Version 1.0.2, 01.05.2003, External Version, Visa International Service Association

VÖB (2002): Aktuelles 2/2002, Bundesverband Öffentlicher Banken Deutschlands

Weltbank (2003): Was ist die Weltbank, www.worldbank.org (09.09.2003)

White (1997): White, L. H. (1997): The Technology Revolution And Monetary Evolution, in: Dorn (1997), S. 15-20

Zederick (1999): Zederick, A. (1999): European Communication Council (ECC) Report: Die Internet-Ökonomie – Strategien für die digitale Wirtschaft, Springer-Verlag, Berlin, Heidelberg, New York

Zeitler (2000): Zeitler, F. (2000): Risikomanagement für Kreditwirtschaft und Finanzmärkte, in Johanning (2000), S. 5-14

Zieschang (2001): Zieschang, T. (2001): Security Engineering im E-Commerce: Best Practices und Standardsicherheitsmaßnahmen, 6. Deutscher IT-Sicherheitskongreß des BSI 2001, Bonn

ZKA (2002): Comments of the Zentraler Kreditausschuss (ZKA) on the Working Document of the European Commission, Internal Market DG „A Possible Legal Framework for the Single Payment Area in the Internal Market“ of 7 May 2002 (MARKT/208/2001 rev.1), Zentraler Kreditausschuss

ZKA (2003a): Zulassung von Terminals im Zahlungssystem GeldKarte der deutschen Kreditwirtschaft, Stand 01.06.2003, Zentraler Kreditausschuss, www.zka.de

ZKA (2003b): Das GeldKarte-System der deutschen Kreditwirtschaft – Ein Systemüberblick, Zentraler Kreditausschuss, www.zka.de