

*Sperrfrist :
29.11.2005, 14.30 Uhr*

**IT IM FINANZSEKTOR
ASPEKTE DER REGULIERUNG UND
ÜBERWACHUNG**

Niklaus Blattner

**Vizepräsident des Direktoriums
der Schweizerischen Nationalbank**

**8. Berner Tagung für Informationssicherheit
Dienstag, 29. November 2005, Bern**

1. Einleitung¹

Am 22. Juni um 17 Uhr 47 stand das gesamte Verkehrsnetz der Schweizerischen Bundesbahnen (SBB) still. Ein Kurzschluss in einer Übertragungsleitung führte zu einer fatalen Kettenreaktion: Die Stromversorgung brach komplett zusammen. Der Stillstand von fast 2'000 Zügen und die Blockierung von rund 200'000 Bahnreisenden waren die Folge.

Ähnlich wichtig wie die Stromversorgung für die SBB ist die Informationstechnologie (IT) für das Finanzsystem. Ein Ausfall der IT-Infrastruktur – an neuralgischen Stellen oder gar flächendeckend – hätte für das Finanzsystem gravierende Folgen. Geht es darum, die Stabilität des schweizerischen Finanzsystems hochzuhalten, nimmt die Gewährleistung der Informationssicherheit eine hohe Priorität ein.

Mein Beitrag zur heutigen Tagung besteht in einem Überblick über den aktuellen Stand der Regulierung und Überwachung der Informationssicherheit im schweizerischen Finanzsektor. Dort, wo ich über die Bankenregulierung spreche, stütze ich mich auf Informationen der Eidgenössischen Bankenkommission (EBK). Dort wo es um die Überwachung der Finanzmarktinfrastrukturen geht, berichte ich über Konzepte und Praxis der dafür verantwortlichen Schweizerischen Nationalbank (SNB).

2. Hintergrund

Das Finanzsystem produziert, überträgt, verarbeitet und speichert in erster Linie Informationen. Diese geben beispielsweise Auskunft darüber, wieviel Geld auf unseren Konten liegt, wem wir wieviel bis wann schulden oder wie sich die Preise der uns interessierenden Wertchriften oder anderer Finanzinstrumente entwickeln. Von besonderer Bedeutung sind Informationen, welche die Abwicklung von Zahlungsaufträgen und das Clearing und Settlement im Effektenhandel ermöglichen. Sind diese Informationen nicht verfügbar, unvollständig oder falsch, reagiert das Finanzsystem empfindlich und kann zum Teil oder ganz zu funktionieren aufhören. Die wirtschaftlichen Folgen solcher Pannen wiegen schwer. Sie bestehen in einer schlagartigen Steigerung der Unsicherheit über Guthaben und Schulden und einem Wegschmelzen der im System vorhandenen Liquidität.

Jederzeit verfügbare, vollständige, integre und nachvollziehbare Daten und deren sichere Verarbeitung sind eine unerlässliche Grundvoraussetzung für das reibungslose Funktionieren des Finanzsystems. Informationssicherheit – verstanden als umfassendes Konzept, das neben der technischen IT-Infrastruktur sämtliche Bereiche abdeckt, die in die Verarbeitung, Übertragung, Speicherung und Sicherung von Informationen involviert sind – ist demzufolge eine zentrale Voraussetzung für die Stabilität eines Finanzsystems.

Dies ist an und für sich nichts Neues. Die Relevanz der Informationssicherheit für die Funktionstüchtigkeit des Finanzsystems hat allerdings in den vergangenen Jahren weiter zugenommen. Dazu trugen verschiedene Faktoren bei, allen voran der technische Fortschritt.

¹ Für die wertvolle Unterstützung anlässlich der Vorbereitung dieses Referats bedankt sich der Verfasser bei Andy Sturm, Prisca Koller und Jürg Mägerle, Organisationseinheit Finanzmarktinfrastuktur, Schweizerische Nationalbank, Zürich.

Prozesse und Systeme wurden weitestgehend automatisiert. Die beträchtlichen Effizienzgewinne setzten immer komplexere Informationssysteme voraus. Die Abhängigkeit von der Technologie wuchs. Die operationellen Risiken nahmen zu.

Ein SBB-Zitat aus dem Jahr 1913 lautet: "...nur... [dank der Selbstversorgung mit Elektrizität] wird die Sicherheit für die Aufrechterhaltung des Bahnbetriebs unter allen Verhältnissen und die Sicherheit der Deckung des Energiebedarfs in der Zukunft erlangt."

Das frühe Streben der SBB nach einer absoluten Unabhängigkeit der Elektrizitätsversorgung war sinnvoll, obgleich die Unabhängigkeit für sich allein genommen natürlich noch keine Versorgungsgarantie mit sich brachte. Analog dazu könnten Finanzinstitute nach einer ähnlichen Unabhängigkeit im IT-Sektor streben. Doch wäre dies keine realistische Option. Während das Stromnetz der SBB vergleichsweise wenige und relativ gut kontrollierbare Schnittstellen zum restlichen Stromnetz der Schweiz aufweist, gewinnen die Informationssysteme im Finanzsektor ihre wirtschaftliche Bedeutung überhaupt erst dadurch, dass sie möglichst alle relevanten Anbieter von Finanzdienstleistungen einschliessen, wobei sich jeder von ihnen mit seinen eigenen Systemen einklinkt.

Erst diese IT-Vernetzung ermöglicht es, das immense Volumen an Finanztransaktionen in hohem Tempo abzuwickeln. Zudem weist die Finanzindustrie auf wirtschaftlicher Ebene eine ganz spezifische Eigenschaft auf: Unternehmungen der Finanzbranche sind gegenseitig ihre grössten Kunden. Die umsatzstärksten Geschäfte einer Bank finden typischerweise mit anderen Banken statt.

Das Pendant der wirtschaftlichen Vorteile solcher Verknüpfungen besteht in einer erhöhten Ausgesetztheit der Informations- und damit der Finanzsysteme gegenüber Kettenreaktionen im Gefolge von IT-Pannen. Dabei ist nicht zu vergessen, dass solche Vernetzungen schon längst die regionalen und nationalen Grenzen überschritten und sich auf internationaler Ebene fortgesetzt haben.

Kettenreaktionen lassen sich anhand eines Beispiels verdeutlichen. Nehmen wir an, dass ein Finanzinstitut aus irgendeinem Grund, sei er operationeller oder technischer Natur, nicht mehr in der Lage ist, Zahlungen auszulösen. Obwohl die betroffene Bank solvent ist und über ausreichende liquide Mittel verfügt, um ihren Zahlungsverpflichtungen nachzukommen, ist sie faktisch zahlungsunfähig. Über den Zahlungsverkehrskanal kann sich diese faktische Zahlungsunfähigkeit auf die mit dem notleidenden Institut verbundenen Banken übertragen. Indem die ihnen zustehenden Gutschriften nicht erfolgen, sie aber trotzdem ihre eigenen Zahlungen auslösen müssen, sinkt ihre Liquidität. Im schlimmsten Fall führt dies zu einem Dominoeffekt, bei welchem nach und nach immer mehr Finanzinstitute zahlungsunfähig werden. Eine solche Kettenreaktion kann sich über weite Teile des Finanzplatzes ausbreiten und ein an sich finanziell gesundes Finanzsystem gesamthaft erschüttern.

Dieses Beispiel illustriert im Übrigen den Begriff der "systemischen Risiken" bzw. der "Systemstabilität" wie er für die SNB massgebend ist. Die SNB trägt die Verantwortung für die jederzeit ausreichende Versorgung der schweizerischen Volkswirtschaft mit Liquidität, d.h. mit Banknoten, Münzen und Buchgeld. Störungen wie die im Beispiel geschilderte, können

die Liquiditätsversorgung gefährden. Gefährdungen der Liquiditätsversorgung setzt die SNB mit Gefährdungen der Systemstabilität gleich. Um die Systemstabilität zu erhöhen, greift die SNB ein, entweder präventiv durch die Regulierung und Überwachung der relevanten Zahlungs-, Effekten- und Devisenabwicklungssysteme oder indem sie im Krisenfall dem Markt zusätzliche Liquidität direkt oder indirekt zur Verfügung stellt.

3. Notwendigkeit der Regulierung?

Finanzinstitute, allen voran die Banken, haben ein starkes, eigenes Interesse an einem angemessenen Sicherheitsniveau. Niemand möchte freiwillig seinen Zahlungsverkehr, seine Guthaben und Verpflichtungen, seine Kreditlinien, seine Devisen- und Effektentransaktionen, seine privaten Ersparnisse, seine Vermögensverwaltung, seine Altersvorsorge usw. einem zweifelhaften Institut überlassen. Das Vertrauen der Kunden in die Sicherheit einer Bank – charakterisiert durch deren Solvenz, Liquidität und Informationssicherheit – ist eine grundlegende Voraussetzung für das erfolgreiche Werben um Kundeneinlagen und das Erbringen aller anderen Dienstleistungen.

Trotzdem können sich die Kunden nicht einfach auf das Eigeninteresse der Banken und auf den zwischen ihnen spielenden Wettbewerb verlassen. Sie müssen sich eine eigene Meinung von deren Vertrauenswürdigkeit bilden. Dies fiel nie leicht. Die zunehmende Verflechtung und Konsolidierung in der Finanzbranche und die sich oft rasch ändernden Verhältnisse machen es eher noch schwieriger, sich ein verlässliches Urteil über den Gesundheitszustand eines Instituts zu bilden.

Die Bankenaufsicht kommt dem Anliegen der Kunden insofern entgegen, als sie die Wahrscheinlichkeit von Bankpleiten vermindert. Gleichzeitig haben die von den Banken veröffentlichten Informationen einem Mindeststandard zu genügen. Auf diese Weise stärkt die Bankenaufsicht das Vertrauen der Bankkunden in die Sicherheit der Institute und fördert die Transparenz gegenüber den Gläubigern und der Öffentlichkeit. Die Verantwortung für die richtige Auswahl der Bank bleibt aber so oder so beim Kunden.

Auch die Betreiber von Zahlungs- und Effektenabwicklungssystemen haben ein starkes Eigeninteresse an sicheren und reibungslos funktionierenden Infrastrukturen. Offensichtlich ist aber auch, dass Investitionen zur Erhöhung der Sicherheit teuer sind. Man denke etwa an die hohen Kosten des Aufbaus und Unterhalts eines Ausweichrechenzentrums. Hier stellt sich ein Anreizproblem: Während die Kosten von den einzelnen Systembetreibern getragen werden müssen, verteilt sich der Nutzen sicherer und zuverlässiger Systeme auf alle, welche die Systeme einsetzen, sei es direkt als Teilnehmer oder indirekt als Kunden der Teilnehmer. Anders formuliert: Von einer höheren Sicherheit eines Zahlungs- bzw. Effektenabwicklungssystems profitieren nicht nur die angeschlossenen Banken und angegliederten Systeme, sondern auch die Bankkunden bzw. die gesamte Volkswirtschaft. Je weiter weg und je weniger klar abgrenzbar die Nutzniesser sind, desto geringer wird ihr Einfluss sein. Hinzu kommt, dass die Kosten relativ leicht zu erfassen sind, während der Nutzen eher diffus bleibt – zumindest, solange keine Krise eintritt. Wir wissen aus Erfah-

rung, dass unter solchen Umständen Märkte zu Unterversorgung neigen – in diesem konkreten Fall eine Unterversorgung mit dem Gut "Sicherheit".

Während die betriebswirtschaftlichen Kosten und Erträge in das unternehmerische Kalkül einfließen, bleiben die volkswirtschaftlichen Kosten und Erträge, die im Falle einer Krise anfallen, unberücksichtigt. Mit anderen Worten: Ein Systembetreiber bemüht sich zwar durchaus um die individuelle Sicherheit – er berücksichtigt aber, solange er scharf kalkuliert, die Folgen, die ein Ausfall für die Stabilität des gesamten Finanzsystems haben könnte, nicht. Aus diesem Grund hat sich in der Schweiz wie auch international die Auffassung durchgesetzt, dass hier der Staat ergänzend das öffentliche Interesse wahrnehmen muss.

4. Regulierung der Informationssicherheit im schweizerischen Finanzsektor

Die EBK beaufsichtigt die in der Schweiz niedergelassenen Banken- und Effektenhändler. Im Zentrum ihrer mikroprudentiellen Aufsichtstätigkeit steht das einzelne Finanzinstitut, insbesondere der Gläubiger- und Anlegerschutz. Aufgabe der SNB ist es demgegenüber, zur Stabilität des Finanzsystems beizutragen, d.h., sie ist makroprudentiell tätig. Im Bereich des Bankensystems trägt die SNB ihrem Gesetzesauftrag insofern Rechnung, als dass sie mittels Stresstests, Frühwarnindikatoren und weiterer Verfahren die Stabilität des Bankensektors als Ganzes evaluiert und auswertet. Ihre Resultate stellt sie auch der EBK zur Verfügung. Diese bezieht sie in ihre eigene Beurteilung ein, trifft gegebenenfalls eigene Massnahmen oder die SNB handelt im Rahmen ihrer eigenen Kompetenzen. Zudem ist die SNB beauftragt, die für das schweizerische Finanzsystem bedeutsamen Zahlungs- und Effektenabwicklungssysteme zu überwachen. Die Aufgaben der EBK und der SNB ergänzen sich also in idealer Weise: Auf der einen Seite steht die EBK, deren Ansatz den Gläubiger- und Anlegerschutz bezweckt, auf der anderen Seite steht die SNB, welche sich nach der Stabilität des Finanzsystems ausrichtet.

Vor diesem Hintergrund wird im Folgenden gezeigt, welche Anforderungen die beiden Behörden an die von ihnen beaufsichtigten bzw. überwachten Institute im Bereich der IT-Sicherheit stellen und wie sie die Einhaltung der Anforderungen durchsetzen.

Institutsaufsicht

Die Bestimmungen zu den Anforderungen an die IT-Betriebsorganisation eines Finanzintermediärs sind in der schweizerischen Bankengesetzgebung relativ allgemein gehalten. Die Vorgaben äussern sich nicht explizit zum Thema Informationssicherheit, sondern sie orientieren sich am Begriff der "einwandfreien bzw. ordnungsgemässen Geschäftsführung". Für die EBK ist die Informationssicherheit nur ein, wenn auch ein wichtiges Anliegen neben anderen. Im eigentlichen Zentrum des Interesses der EBK steht die finanzielle Robustheit der Banken, d.h. deren Solvenz. Ein Blick auf die entsprechenden bankengesetzlichen Bestimmungen zeigt, dass die Konkretisierung der Anforderungen an

die Informationssicherheit hingegen oftmals den internen und externen, gesetzlichen Revisionsstellen überlassen bleibt.

Zu verschiedenen kritischen Bereichen hat sich die EBK allerdings in Rundschreiben näher geäußert, so z.B. zur externen Datenverarbeitung und zum Outsourcing.² Die EBK definiert Outsourcing als die Auslagerung von *wesentlichen* Geschäftsbereichen aus einer von ihr beaufsichtigten Bank an eine andere Unternehmung, den Dienstleister. Als "wesentlich" gelten Bereiche, welche sich insbesondere auf die Erfassung, Begrenzung und Überwachung von Markt-, Kredit-, Ausfall-, Abwicklungs-, Liquiditäts- und Imagerisiken sowie auf operationelle und rechtliche Risiken auswirken (Rz. 2). Das Outsourcing nimmt im IT-Bereich eine besondere Stellung ein. Das behördliche Interesse am Outsourcing gründet darin, dass eine Bank im Zuge des Outsourcing einen für ihre Geschäftstätigkeit zentralen Bereich in eine nicht regulierte Unternehmung auslagern und somit der Bankenaufsicht entziehen könnte, was nicht hingenommen werden darf, wenn die Aufsicht über die Banken nicht verwässert werden soll. Deshalb wird im Rundschreiben über die Auslagerung von Geschäftsbereichen der Grundsatz festgehalten, dass Outsourcing jedes (wesentlichen) Geschäftsbereichs zwar ohne Bewilligung durch die EBK möglich ist (Rz. 13). Voraussetzung dafür sind aber die Einhaltung des Bundesgesetzes über den Datenschutz und die Einhaltung der im Rundschreiben aufgeführten Anforderungen an ein sicheres Outsourcing. Beispielsweise müssen Kundendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Rz. 30). Kann eine Bank diese Anforderungen nicht erfüllen, muss sie vor der Auslagerung der EBK ein begründetes Gesuch für eine Abweichung einreichen (Rz. 14). Ausserdem trägt das auslagernde Institut gegenüber der EBK weiterhin die Verantwortung für den ausgelagerten Geschäftsbereich. Outsourcingbeispiele im IT-Bereich, die vom EBK-Rundschreiben tangiert werden, sind etwa: der Betrieb von IT-Systemen, die Datenaufbewahrung und der Betrieb und Unterhalt von Datenbanken; im Bereich des Wertschriftenhandels wird zum Beispiel die Wertschriftenverwaltung als wesentliche Dienstleistung verstanden. Die bankengesetzliche Revisionsstelle hat die Einhaltung der Anforderungen jährlich zu prüfen und die Prüfergebnisse in ihrem Prüfbericht an die EBK festzuhalten.

Das EBK-Rundschreiben regelt nur die Frage, unter welchen Umständen ein Outsourcing zulässig ist. Die Bedingungen, welche die externen Dienstleister hinsichtlich der IT-Sicherheit erfüllen müssen, werden im Rundschreiben nicht präzisiert. Die Anforderungen an die Informationssicherheit werden durch die externen Revisionsstellen spezifiziert. Um diesen Ansatz zu verstehen, lohnt es sich, sich in Erinnerung zu rufen, dass das Universum der von der EBK beaufsichtigten Institute sehr heterogen ist. Anforderungen, die für eine kleine Sparkasse sinnvoll sind, genügen für eine Grossbank sicher nicht. Umgekehrt führen Anforderungen, die für eine Grossbank angemessen sind, bei kleineren Banken schon bald zu einem "regulatory overkill". Das von der EBK praktizierte dualistische Aufsichtssystem begünstigt auch hier eine institutsspezifische Umsetzung relativ allgemein gehaltener Anforderungen. Die von der EBK angestrebte verstärkte Risikoorientierung bei der banken-

² Rundschreiben der Eidg. Bankenkommission: Auslagerung von Geschäftsbereichen (Outsourcing) vom 26. August 1999 (letzte Änderung: 29. Juni 2005) - EBK-RS 99/2 Outsourcing.

gesetzlichen Revisionstätigkeit dürfte ausserdem zur Folge haben, dass die Prüfungsgesellschaften den Risiken im Bereich der Informationssicherheit in Zukunft zusätzliche Aufmerksamkeit schenken werden.

Systemüberwachung

Das neue Nationalbankgesetzes (NBG) und die dazugehörige Nationalbankverordnung (NBV) traten im Mai 2004 in Kraft. Damit wurde in der Schweiz die rechtliche Grundlage zur Überwachung systemisch relevanter Finanzmarktinfrastrukturen formalisiert. Das Mandat der SNB ist auf die Geschäftsabwicklung im Zahlungsverkehr und im Wertschriftenbereich beschränkt; der Börsenhandel fällt nicht darunter. Ganz im Sinne des Schutzobjekts – der Stabilität des Finanzsystems – konzentriert sich die Überwachung auf jene Systeme, von denen eine potenzielle Gefährdung der Stabilität des schweizerischen Finanzsystems ausgeht. In einem ersten Schritt hat die SNB deshalb jene Systeme identifiziert, die sie als *systemisch bedeutsam* einstuft. Es sind dies das Zahlungssystem Swiss Interbank Clearing (SIC), das Wertschriftenabwicklungssystem SECOM, die dem Börsenhandel nachgelagerte zentrale Gegenpartei x-clear und das internationale Devisenabwicklungssystem Continuous Linked Settlement (CLS).

Mit Ausnahme von CLS, welches bereits durch das NY-Fed überwacht wird, müssen die Betreiber dieser Infrastrukturen die in der NBV festgelegten Mindestanforderungen erfüllen (NBV Art. 22 – 34). Die Informationssicherheit spielt dabei eine zentrale Rolle. Die NBV enthält Anforderungen, die sich auf die Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit von Daten respektive Informationen beziehen. Insbesondere ist festgehalten, dass das System für den gesamten Verarbeitungsprozess hinsichtlich dieser Kriterien hohen Sicherheitsanforderungen genügen und dass sich der Systembetreiber an anerkannten Standards orientieren muss.

Allerdings sind die Mindestanforderungen auch auf Verordnungsstufe noch relativ allgemein formuliert. In den vergangenen Monaten hat die SNB deshalb eine Konkretisierung der Anforderungen vorgenommen. Mit den konkretisierten Anforderungen – Control Objectives – werden zwei Ziele verfolgt. Die Konkretisierung der Anforderungen soll den Betreibern erstens erleichtern, sie einzuhalten. Zweitens sollen sie der SNB die Überprüfung der Einhaltung erleichtern.

Die Control Objectives sind weitgehend zielorientiert formuliert. Um möglichst wenig in die operative Tätigkeit der Betreiber einzugreifen, schreiben sie nicht vor, auf welche Art und Weise ein erwünschter Zustand erreichen soll, sondern es wird lediglich das Sicherheitsziel vorgegeben.

Die Control Objectives sind thematisch dreigeteilt. Ein erster Teil beinhaltet allgemeine Anforderungen an die Unternehmensführung (Governance) und an die einem System zu Grunde liegenden vertraglichen Grundlagen. In einem zweiten Teil sind die Anforderungen bezüglich Risikoanalyse, Risikomanagement und Risikokontrolle zur Eingrenzung der Kredit- und Liquiditätsrisiken zusammengefasst. Der dritte und umfangreichste Teil enthält die Anforderungen im Bereich der Informationssicherheit.

Die Zielvorgaben für die Informationssicherheit decken unter anderem die folgenden Aspekte ab: Sicherheitspolitik und -organisation, personelle und physische Sicherheit, Systembetrieb, Systementwicklung und -wartung, Kommunikation und Informationsaustausch, und – last but not least – das Kontinuitätsmanagement (Business Continuity Management). Selbstverständlich hatten die Systembetreiber die Gelegenheit, im Rahmen einer Vernehmlassung zu den Control Objectives Stellung zu nehmen. Zur Zeit werden die Details bereinigt, sodass einer Verabschiedung der Control Objectives noch vor Ende des Jahres nichts entgegen stehen sollte.

Wie beabsichtigt die SNB, die Einhaltung der genannten Anforderungen zu überprüfen? Grundsätzlich verfolgt die SNB ähnlich wie die EBK einen dualistischen Ansatz, d.h., sie wird sich bei ihrer Beurteilung überwiegend auf die Analysen und Prüfergebnisse der internen Revision und externer Prüfgesellschaften abstützen. Dabei muss die externe Prüfgesellschaft innerhalb eines dreijährigen Revisionszyklus zu jedem Control Objective Stellung nehmen. Tiefe und Intensität der jeweiligen Prüfungen hängen in erster Linie von einer vorangehenden Risikoanalyse ab. Neben diesen regulären Prüfungen kann die SNB im Bedarfsfall auch Sonderprüfungen veranlassen. Solche ausserordentlichen Prüfungen kommen allerdings nur zum Einsatz, wenn die SNB über hinreichende Indizien verfügt, wonach ein Systembetreiber einem wesentlichen Risiko ausgesetzt ist.

Zwischen der Überwachung der SNB und der Aufsicht der EBK bestehen sowohl Gemeinsamkeiten als auch Unterschiede. Gemeinsam ist beiden das dualistische Aufsichts- bzw. Überwachungskonzept und die Risikoorientierung. Ein Unterschied besteht in der Konkretisierung der Anforderungen, die bei der Systemüberwachung, d.h. bei der Überwachung der Informationssicherheit von Finanzmarktinfrastrukturen, wesentlich detaillierter ausgefallen ist. Dafür sprechen zwei Gründe. Erstens konzentriert sich die SNB auf einen kleinen und homogenen Kreis von Systembetreibern. Die Anforderungen können hier – ganz im Gegensatz zur heterogenen Gruppe der Banken – massgeschneidert werden. Zweitens handelt es sich bei den Systembetreibern im Wesentlichen um IT-Dienstleister, d.h., die Informationssicherheit spielt eine zentrale Rolle. Dies steht im Kontrast zu den Finanzinstituten, deren Risikoprofil viel breiter ist, was ebenfalls nach allgemeiner gehaltenen Vorschriften ruft.

Sektorübergreifende Massnahmen

Sowohl die EBK als auch die SNB tragen der Informationssicherheit in ihrer Regulierung, Aufsicht und Überwachung Rechnung. Im Mittelpunkt stehen die Vorkehren, welche auf der Stufe der einzelnen Finanzinstitute bzw. Systembetreiber getroffen werden.

Zusätzlich stellen sich allerdings auch Fragen, welche sich aus den vielfältigen Interdependenzen zwischen den Finanzmarktakteuren ergeben. Im Krisenfall werden diese Zusammenhänge am spürbarsten. Deshalb braucht es gerade für die erfolgreiche Bewältigung von grösseren, unvorhergesehenen Störfällen weitere vorkehrende Massnahmen. Diese werden zwar je einzeln durch die Institute oder Betreiber umgesetzt. Sie müssen aber von allen wichtigen Akteuren gemeinsam, sozusagen übergeordnet koordiniert und abgestimmt werden, wenn sie erfolgversprechend sein sollen.

Gestützt auf einen Entscheid der Projektgruppe "Gemeinschaftswerke Finanzplatz Schweiz", welche durch die Schweizerische Bankiervereinigung ins Leben gerufen wurde, hat sich vor ziemlich genau zwei Jahren eine "Steuerungsgruppe Business Continuity Planning" konstituiert, welche unter der Leitung der SNB eine Überprüfung und Beurteilung der in den einzelnen Unternehmen erarbeiteten Business Continuity Pläne vornahm. In dieser Steuerungsgruppe vertreten waren neben der SNB auch die EBK, Credit Suisse, PostFinance, UBS, SIS, SWX und Telekurs.

Der Bericht der Steuerungsgruppe wird in Kürze veröffentlicht, weshalb ich an dieser Stelle nicht auf alle Einzelheiten eingehe. Folgende drei Punkte scheinen mir aber besonders erwähnenswert. Erstens zeigt der Bericht auf, dass die systemisch bedeutsamen Infrastrukturen und deren wichtigste Teilnehmer in ihren BCP-Bemühungen weit fortgeschritten sind. Zweitens einigte sich das Steuerungsgremium auf konkrete Vorgaben, an welchen sich die verschiedenen Akteure bei ihrem Business Continuity Planning zu orientieren haben. So gilt für die kritischen Zahlungs- und Effektenabwicklungssysteme eine maximale Ausfallzeit von zwei Stunden; für wichtige Systemteilnehmer beträgt die tolerierte Ausfallzeit vier Stunden. Innerhalb dieser Zeitspanne sollten sie in der Lage sein, ihre kritischen Geschäftsprozesse wieder aufzunehmen, sei es über die normalen Kanäle oder via Alternativprozesse. Diesen Anforderungen liegt das Szenario des Ausfalls eines betriebswichtigen Gebäudes, einschliesslich der darin tätigen Mitarbeitenden, zu Grunde. Drittens identifiziert der Bericht in verschiedener Hinsicht Verbesserungspotenzial. Eine Massnahme, die inzwischen bereits umgesetzt ist, betrifft die Schaffung einer finanzsektorübergreifenden Alarm- und Krisenorganisation. Die vorliegenden Analysen zeigen auch, dass die meisten Institute im Bereich der technischen Einrichtungen zwar gut auf das beschriebene Szenario vorbereitet sind. Hingegen besteht häufig ein Mangel an sachkundigen Mitarbeitenden, welche im Krisenfall sehr kurzfristig die betrieblichen Funktionen übernehmen könnten. Im Rahmen der Umsetzung verschiedener Empfehlungen sind die einzelnen Institute deshalb angehalten, angemessene Betriebskonzepte zur Lösung der Loss-of-staff-Problematik zu entwickeln und einzuführen. Informationssicherheit ist nicht nur eine Frage von Hard- und Software, sondern hängt nicht zuletzt von den Menschen ab, welche sich für sie einsetzen.

5. Schlussbemerkungen

Die schweizerischen Aufsichts- und Überwachungsbehörden schenken dem Aspekt der Informationssicherheit grosse und zunehmende Aufmerksamkeit. Dasselbe sollten wir auch für die Unternehmen im Finanzsektor selbst sagen können. Und hier wende ich mich an die Vertreter von Finanzdienstleistungsunternehmen und –infrastrukturen unter Ihnen.

Ausgangspunkt ist der Grundsatz, dass die Verantwortung für die Gewährleistung der Informationssicherheit primär bei den einzelnen Unternehmen liegt. Regulierung, Aufsicht und Überwachung spielen nur eine ergänzende Rolle. Das Thema Informationssicherheit verdient daher in jedem Verwaltungsrat und jeder Geschäftsleitung eine angemessene Priorität, unabhängig davon, ob es sich nun um einen Global Player oder um eine kleine Sparkasse handelt. Um die Informationssicherheit dauerhaft zu gewährleisten, bedarf es konti-

nuierlicher Anstrengungen. Dafür verantwortlich ist die rasante technologische Entwicklung. Hinzu kommen die erforderlichen Anpassungen an die häufigen Restrukturierungen der Unternehmen und die Notwendigkeit, die Tauglichkeit der Konzepte regelmässig im Rahmen von Übungen zu überprüfen. Nur so kann vermieden werden, dass dem Schweizer Finanzplatz Ereignisse wie sie z.B. die SBB jüngst verkraften mussten, erspart bleibt.