BASEL COMMITTEE ON BANKING SUPERVISION

BANK FOR INTERNATIONAL SETTLEMENTS

Risiken in EDV- und Telekommunikationssystemen

(Juli 1989)

Die rasanten technischen Neuentwicklungen im Bereich von EDV und Telekommunikation in den letzten Jahren sowie die Integration automatisierter Transaktionen verstärken die Abhängigkeit der Banken von der Zuverlässigkeit und der ständigen Betriebsbereitschaft ihrer EDV-Systeme.

Die Banken waren seit jeher Fehler- und Betrugsrisiken ausgesetzt, dramatisch verändert haben sich allerdings der Umfang dieser Risiken und die Geschwindigkeit, mit der sie auftreten können. Infolge der automatisierten Abwicklungssysteme besteht darüber hinaus ein weltumspannendes, dichtes Netzwerk von Interbankkreditbeziehungen. Sobald eine Bank wegen Systemproblemen, wegen Zahlungsunfähigkeit oder aus anderen Gründen eine Zahlung nicht leisten kann, haben die Banken, die der betreffenden Bank Kredit gewährt haben, ebenfalls Zahlungsschwierigkeiten, so dass sich die Zahlungsunfähigkeit in einer Kettenreaktion durch das ganze System fortpflanzt und die Gefahr besteht, dass sie das gesamte Abwicklungssystem erfasst und lahmlegt.

Die für ein EDV-Umfeld typischen Risikoarten sowie die notwendigen Sicherheits- und Kontrollvorkehrungen erfordern die volle Aufmerksamkeit der Aufsichtsbehörden. In diesem Papier werden die folgenden Risikoarten behandelt: Kenntnisnahme von Informationen durch Unbefugte, Fehler, betrügerische Machenschaften, Störung des Geschäfts wegen Hardware- oder Software-Pannen, unzulängliche Planung sowie Risiken im Zusammenhang mit der EDV-Tätigkeit der Endbenutzer.

Dieses Papier wurde als Nachschlagewerk für die Aufsichtsbehörden eines breiten Spektrums von Rechtsordnungen verfasst. Es richtet sich nicht an technische Fachleute, sondern soll vielmehr die wichtigsten Problembereiche hervorheben, die die Aufsichtsbehörden kennen müssen.

Kenntnisnahme von Informationen durch Unbefugte

In einer Bank werden die meisten Informationen durch elektronische Datenverarbeitung generiert oder sind direkt damit verknüpft. Daten und Dokumente zirkulieren routinemässig innerhalb einer Bank oder werden zwischen der Bank und ihren Korrespondenten und Kunden über öffentliche Telekommunikationsverbindungen wie Telefonleitungen und Satelliten weitergegeben. Zahlreiche Benutzer, darunter Angestellte und Bankkunden, können über Computerterminals oder über das Telefon direkt auf diese Daten zugreifen. Dadurch werden zwar die Dienstleistungen für die Kunden verbessert und die internen Transaktionen erleichtert, es wächst jedoch auch die Gefahr von Fehlern und Missbrauch der Informationen der Bank.

Die in einer Bank anfallenden Informationen sind zu einem grossen Teil vertraulich; wenn sie in falsche Hände fallen, können die Kundenbeziehungen und der Ruf der Bank Schaden leiden, und es können Schadensersatzforderungen erhoben werden. Beispiele für solche Informationen sind der Stand von Kundenkonten, Überziehungslimits und Einzelheiten zu Transaktionen. Korrespondenz und Strategiepapiere werden in Textverarbeitungssystemen ebenfalls elektronisch verfasst und gespeichert. In EDV-Systemen besteht im Vergleich zu manuellen Systemen ein erhöhtes Risiko einer Kenntnisnahme vertraulicher Informationen durch Unbefugte, weil ihnen viel grössere Datenmengen in einer praktischeren und leichter zu bearbeitenden Form (z.B. Kopien auf Magnetbändern oder Disketten) entnommen werden können und ein unbefugter Zugriff möglicherweise keine Spuren hinterlässt.

Zum Schutz der Bank sind daher angemessene Sicherheits- und Kontrollvorkehrungen erforderlich. Der Umfang der Kontrollen ist dabei gegen den Grad des Risikos und die Auswirkungen eines Verlusts (oder einer Offenlegung) für die Bank abzuwägen.

Für die Informationssicherheit bestehen u.a. folgende technische Kontrollen: Verschlüsselung (Text wird in Reihen sinnloser Symbole umgewandelt), Beglaubigungscodes für Nachrichten (dabei soll ein bestimmter Code vor unbefugter Änderung elektronischer Daten während der Übermittlung oder der Speicherung schützen) sowie der Einsatz von Sicherheitsanwendungen, mit deren Hilfe der Zugang zu Daten, Dateien, Programmen, Hilfsfunktionen und Systembefehlen in Rechnern eingeschränkt

wird. Solche Systeme können den Zugang nach Benutzer, nach Transaktion oder nach Terminal kontrollieren. Verstösse gegen die Sicherheit, einschliesslich des Versuchs dazu, können gemeldet werden.

Fehler

Fehler treten in der Regel und sehr häufig beim Erfassen von Daten und beim Entwickeln und Ändern von Programmen auf. Erhebliche Fehler können auch bei der Systemgestaltung, bei routinemässigem „Aufräumen“ im System sowie bei der Verwendung spezieller Programme zur Behebung anderer Fehler auftreten. Die Ursache ist in der Regel menschliches Versagen; es kommt relativ selten vor, dass ein Fehler durch das Versagen elektronischer oder mechanischer Systemkomponenten verursacht wird. Ausserdem können sich Fehler in Software-Pakete einschleichen, wenn diese speziell auf die Bedürfnisse eines bestimmten Benutzers zugeschnitten werden. Beim Einkauf von Standard-Software sollte daher darauf geachtet werden, möglichst wenig Änderungen daran vorzunehmen.

Betrügerische Machenschaften

Die Datenströme im Bankgeschäft stellen Vermögenswerte dar oder Instruktionen, mit denen letztlich Vermögenswerte verschoben werden. Die Geschwindigkeit, mit der Vermögenswerte mittels elektronischer Zahlungs- und Nachrichtenaustauschsysteme übertragen werden können, erschwert die Aufgabe der internen Kontrolle. Erfolgreiche betrügerische Machenschaften führen nicht nur zu einem direkten finanziellen Verlust für die Bank, sondern beeinträchtigen das Vertrauen in die Bank und ganz allgemein in das Bankgewerbe, wenn sie in den Medien gemeldet werden. Die vielfältigen Zugangswege zu EDV-Aufzeichnungen eröffnen zahlreiche Möglichkeiten für betrügerische Machenschaften, z.B.:

- Es können missbräuchlich Transaktionen in das EDV-System eingegeben werden.
- Während routinemässiger Entwicklungs- oder Wartungsarbeiten können an Programmen unbefugterweise Änderungen vorgenommen werden, die dazu führen, dass das Programm automatisch betrügerische Transaktionen durchführt, Kontrollmechanismen bei ausgewählten Konten ignoriert oder die Aufzeichnung bestimmter Transaktionen löscht.
- Mit speziellen Programmen können missbräuchliche Änderungen der elektronischen Aufzeichnungen vorgenommen werden, wobei die üblichen Kontrollmechanismen und Prüfungspfade, die in die EDV-Systeme eingebaut sind, umgangen werden.
- Dateien können physisch aus dem Rechner entfernt, durch Einfügen betrügerischer Transaktionen oder Salden geändert und für die Verarbeitung zurückgebracht werden.
- Transaktionen können auf betrügerische Weise eingeführt oder abgefangen und geändert werden, während sie über Telekommunikationsnetze übermittelt werden.

Derzeit werden neue Zahlungsformen eingeführt, die es Dritten ermöglichen, über EDV-Einrichtungen Zahlungen einzuleiten. Betrügerische Machenschaften, bei denen unbefugter Zugang zu Telekommunikationsnetzen eine Rolle spielt, dürften daher noch zunehmen.

Die meisten im Bankgeschäft verwendeten Systeme enthalten Kontrollmechanismen und erstellen Meldungen, die bei der Verhütung oder Aufdeckung solcher betrügerischer Machenschaften helfen sollen. Auch diese können jedoch unter Umständen von Personen manipuliert werden, die Zugang zu Computerterminals oder -dateien haben.

Beim Aufbau wirksamer interner Kontrollsysteme ist es daher sehr wichtig, sämtliche Schwachstellen aller Systeme zu erkennen. Wichtige Aufzeichnungen und Programme sind besonders gegen unbefugte Änderungen zu schützen. Ferner ist darauf zu achten, dass die Mitarbeiter in den kritischen Bereichen sorgfältig geschult werden und dass eine angemessene Aufgabentrennung besteht.

Störungen des Geschäfts wegen Hardware- oder Software-Pannen

EDV-Systeme bestehen aus zahlreichen Hardware- und Software-Komponenten, und beim Versagen irgendeiner dieser Komponenten kann das ganze System abstürzen. Oft konzentrieren sich diese Komponenten auf einen einzigen oder einige wenige Standorte, so dass sich eine Störung besonders stark auswirken kann.

Früher griff man bei Versagen von EDV-Systemen auf die manuellen Verfahren zurück, die vom EDV-System abgelöst worden waren. Dieses Vorgehen ist jedoch jetzt meist nicht mehr praktikabel - nur noch wenige Banken könnten ohne EDV-Systeme arbeiten. Die Verarbeitung und Weitergabe von Informationen mittels immer besserer Technologie hat die Abhängigkeit der Geschäftsleitung von der Verfügbarkeit und Zuverlässigkeit automatisierter Systeme verstärkt. Die ständige Verfügbarkeit der Informationssysteme einer Bank ist ein unverzichtbarer Bestandteil eines effizienten Entscheidungsprozesses der Geschäftsleitung.

Wenn ein EDV-System ausser Betrieb ist, tritt der Schaden bei den Echtzeit-Bankdienstleistungen für die Kunden unverzüglich ein und wächst rasch. Schnell häufen sich Verarbeitungsrückstände an, und nach einer Betriebsunterbrechung von mehreren Stunden kann es tagelang dauern, diese Rückstände aufzuarbeiten. Besonders verheerend sind die Folgen bei elektronischen Überweisungs- und Zahlungssystemen, insbesondere denjenigen mit garantierter Abwicklung am selben Tag, da die Begünstigten sich dort darauf verlassen, dass sie die Mittel erhalten, die sie zur Begleichung ihrer eigenen Verbindlichkeiten benötigen. Die Folgekosten eines grösseren Systemausfalls können die Kosten für den Ersatz beschädigter Hardware, Daten oder Software bei weitem übersteigen.

Eine leistungsfähige Notfallplanung ist ein Weg, auf dem die Geschäftsleitung die Konsequenzen derartiger Betriebsprobleme mildern kann. Diese Planung sollte Teil des internen Kontrollsystems und der physischen Sicherheitsvorkehrungen einer Bank bilden. Sie sollte Vorkehrungen für die Weiterführung der Geschäfte und für die Wiederaufnahme des Betriebs nach einer Störung oder einem Zusammenbruch der Systeme der Bank enthalten. Zu diesem Zweck sollten Duplikate wichtiger Dateien, von Software und von Hardware an einem Standort ausserhalb der Bank sowie andere Möglichkeiten der Informationsverarbeitung vorgesehen sein. In regelmässigen Abständen ist zu prüfen, ob die Notfallplanung einer Bank noch aktuell ist. Wenn eine Bank für ihre Datenverarbeitung einen aussenstehenden EDV-Dienstleistungsanbieter in Anspruch nimmt, muss sie sich vergewissern, dass die Notfallplanung dieses Anbieters ihre eigene ergänzt.

Unzulängliche Planung

Eine solide Planung ist von wesentlicher Bedeutung. Die Effizienz einer Bank und die Qualität ihrer Dienstleistungen hängen heutzutage derart stark von EDV-Systemen ab, dass ein Versagen bei der Planung oder Entwicklung neuer Systeme erhebliche geschäftliche Folgen haben kann. Kann eine Bank neue Systeme und Dienstleistungen nicht schnell genug einführen, stellt dies oft einen erheblichen Wettbewerbsnachteil dar. Andererseits hat sich eine EDV-Umstellung um jeden Preis, vor allem bei verhältnismässig geringem Nutzen, schon oft als kostspieliger Fehler erwiesen.

Einige Finanzinstitute waren mit erheblichen Problemen konfrontiert, als sie versuchten, umfassende integrierte Systeme für Finanzgeschäfte einzuführen. In einem integrierten Software-System bilden Programme für verschiedene Anwendungen - Kredite, Einlagen, Klein- und Grosskunden -, die normalerweise als selbständige Programme konzipiert und betrieben werden, von Anfang an Teile eines Ganzen. Mit diesem Ansatz sollen die Aktualität der Informationen erhöht, die Leistungsfähigkeit gefördert und die Einführung neuer Produkte erleichtert werden. In einigen Fällen wurden die Kosten, der Zeitaufwand und die Personalressourcen, die für die erfolgreiche Installierung integrierter Systeme benötigt werden, unterschätzt. Über viele Jahre hinweg entwickelte Projekte wurden aufgegeben, nachdem sie enorme Kosten verursacht hatten.

Angesichts der Komplexität von EDV-Systemen und ihres Einflusses in der gesamten Organisation ist für das Gelingen jedes Projekts das Engagement der obersten Ebene der Geschäftsleitung erforderlich. Die Geschäftsleitung sollte der langfristigen (strategischen) Planung der EDV-Systeme, der Hard- und Software, Machbarkeitsstudien, Spezifikationen der Systeme, der Auswahl der Lieferanten und der Projektkontrolle viel Aufmerksamkeit widmen.

Risiken im Zusammenhang mit der EDV-Tätigkeit der Endbenutzer

Bis vor kurzem spielten Personal Computer (PCs), Mikrocomputer und sonstige Rechnergeräte für Endbenutzer nur eine relativ unbedeutende Rolle in der gesamten EDV-Tätigkeit. Jetzt aber haben die technischen Vorzüge, die Zweckdienlichkeit und die Kostenvorteile der individuellen Datenverarbeitung den Einsatz solcher Geräte stark ansteigen lassen, so dass ein Teil der Datenverarbeitung aus dem zentralisierten Kontrollumfeld herausgenommen wurde. Risiken im Zusammenhang mit der EDV treten nun in neuen Bereichen einer Bank auf, und sehr oft sind für diese EDV-Tätigkeiten nicht einmal elementare Kontroll- und Überwachungsmechanismen eingeführt worden. Das Hauptproblem bei der individuellen Datenverarbeitung besteht darin, dass diese neuen Netze zur Informationsübermittlung und -verarbeitung weit schneller eingeführt werden als die entsprechenden Kontrollen.

Die Risiken sind im allgemeinen dieselben wie bei Grossrechnern, besondere Aufmerksamkeit ist jedoch der Möglichkeit von Korruption oder Verlust von Daten oder Software und der damit verbundenen Beeinträchtigung des reibungslosen Funktionierens des gesamten Betriebsnetzes der Bank zu widmen. Mikrocomputer werden heutzutage nicht nur für die Textverarbeitung verwendet, sondern auch zur Kommunikation mit anderen Rechnern und als selbständige Datenverarbeitungsgeräte. Da diese Systeme oft sehr individuell gestaltet und unabhängig sind und oft eine einzige Person die volle Verantwortung für die Entwicklung, die Erprobung, die Einführung und den Betrieb eines Programmpakets trägt, wächst die Gefahr, dass Verfahren und Datenbearbeitungsmethoden verwendet werden, die sich vom Standard in der übrigen Bank unterscheiden und mit diesem nicht kompatibel sind.

Verantwortung der Geschäftsleitung

Es ist Aufgabe der Geschäftsleitung, dafür zu sorgen, dass der Betrieb angemessen gegen die oben beschriebenen Risiken geschützt ist. Als ersten Schritt sollte die Geschäftsleitung geeignete *Verhütungsmassnahmen* ergreifen, die die Wahrscheinlichkeit, dass einer der beschriebenen Risikofälle tatsächlich eintritt, auf ein Minimum reduzieren. Solche Verhütungsmassnahmen sind z.B. die sorgfältige Gestaltung und Standortwahl von Rechnerzentren, Dateneingabekontrollen, Sicherheitsmassnahmen zur Verhinderung unbefugten Zugangs zu Rechnerausrüstungen sowie Passwörter für die Einschränkung des Zugriffs auf Computerprogramme und Daten.

Da Verhütungsmassnahmen nie einen hundertprozentigen Schutz bieten können, sollte die Geschäftsleitung darüber hinaus Systeme zur *Schadensbegrenzung* entwickeln. Diese müssen so gestaltet sein, dass sie die Auswirkungen von Störungen, die von den präventiven Kontrollen nicht abgefangen werden und die den Geschäftsbetrieb der Bank bedrohen, aufspüren und begrenzen. Solche Massnahmen sind u.a. die Duplizierung von Telekommunikations- und EDV-Netzen als Sicherheitsvorkehrung bei Zusammenbrüchen, Abstimmungsverfahren zur Fehlererkennung sowie Katastrophenpläne. Eine spezielle Schadensbegrenzungsmassnahme, die eine sorgfältig gestaltete EDV-Politik ergänzt, ist eine Versicherung gegen Verluste durch betrügerische Machenschaften von Angestellten, für die Kosten der Wiederbeschaffung von Daten sowie gegen die Zerstörung von Soft- oder Hardware.

Interne Revision

Das Verwaltungsorgan und die Geschäftsleitung sind ausserdem dafür verantwortlich, die EDV-Kontrollsysteme zu überprüfen, zu überwachen und zu testen, um sicherzustellen, dass sie im täglichen Betrieb wirksam und für die Geschäftsvorgänge nach wie vor relevant sind. Regelmässig sind unabhängige Tests der Sicherheits- und Kontrollverfahen durch interne und externe Revisoren oder durch Berater vorzusehen. Mit einem solchen Testprogramm sollten Lücken in den Kontrollmechanismen rechtzeitig entdeckt werden können, bevor eine ernsthafte Gefahr für den Bankbetrieb entsteht. Die Häufigkeit und Gründlichkeit der von den Revisoren in irgendeinem Bereich durchgeführten Tests sollten dem Grad des Risikos Rechnung tragen, das für die Bank besteht, wenn die Sicherheits- und Kontrollvorkehrungen im betreffenden Bereich versagen.

Massnahmen der Aufsichtsbehörden

Aus der Sicht der Aufsichtsbehörden ist es notwendig, sowohl die Angemessenheit der EDV-Politik eines Finanzinstituts zu beurteilen als auch die Leistungsfähigkeit seiner internen EDV-Kontrollen und Revisionsverfahren. Die Aufsichtsbehörde kann ihrer Verantwortung u.a. dadurch nachkommen, dass sie sich mittels eines *Fragebogens* oder mittels Meldungen einen Überblick über die Situation verschafft, häufiger aber fällt dies in die Zuständigkeit der externen oder internen Revisoren. Ein einfacher Fragebogen oder eine Meldung genügt in der Regel, um der Aufsichtsbehörde einen ersten Überblick zu gewähren, sollte jedoch nicht als Ersatz für eine gründliche Prüfung durch die EDV-Sicherheits- oder Revisionsspezialisten angesehen werden. Das Thema ist technisch komplex, und in jeder Bank besteht eine grosse Bandbreite von Schwachstellen und Kontrolltechniken unter den verschiedenen Hardware- und Software-Typen.

In einem derart spezialisierten Bereich ist die Aufsichtsbehörde gut beraten, wenn sie das Fachwissen der *externen Revisoren* in Anspruch nimmt. Diese sollten ermutigt werden, für diesen Teil ihrer Aufgabe genügend Ressourcen einzusetzen.

Es empfiehlt sich, die Aufmerksamkeit der externen Revisoren auf diesen Bereich zu lenken und die Banken zu ersuchen, im Revisionsauftrag auch festzuhalten, dass die Revisoren periodisch die Solidität der für den Geschäftsbetrieb der Bank wichtigsten EDV-Verfahren sowie die Wirksamkeit der internen EDV-Kontrollen überprüfen müssen. Die externen Revisoren sollten ausserdem aufgefordert werden, in ihrem jährlichen Bericht an die Geschäftsleitung auf etwaige Mängel und Schwachstellen hinzuweisen, die sie im Rahmen ihrer Prüfung dieses besonderen Bereichs festgestellt haben.

Wenn die Aufsichtsbehörde ihre Verantwortung hauptsächlich mittels *Prüfungen vor Ort* wahrnimmt, gehört es zum ordentlichen Verfahren, dass die Inspektoren Besprechungen, Prüfungen von Unterlagen und Stichprobenkontrollen in diesem Bereich vornehmen. Ein begrenzter Personalbestand und begrenztes Fachwissen, neben finanziellen und sonstigen Einschränkungen, erschweren es allerdings den Inspektoren, mit der Entwicklung neuer EDV-Systeme Schritt zu halten. Es ist jedoch unbestreitbar sehr wichtig, dass den Inspektionsteams EDV-Spezialisten angehören, deren Ausbildung der fortgeschrittenen EDV-Technologie in den geprüften Banken entspricht.

Bei ihrer Arbeit im EDV-Bereich benutzen sowohl die Inspektoren als auch die Revisoren in der Regel Checklisten oder Prüfungshandbücher, die von der Aufsichtsbehörde in Zusammenarbeit mit spezialisierten Institutionen erstellt wurden, und diese bilden ein äusserst nützliches Aufsichtsinstrument.