

# Frühzeitig vorbeugen

**Business Continuity Management** ■ Schutz vor Terroranschlägen ist das Thema in der globalen Finanzindustrie. Die heute von Terroristen verwendeten archaischen Methoden sind zwar mörderisch brutal, aber zumindest regional begrenzt. Dies könnte sich schlagartig ändern, wenn unsere Informatik- und Telekommunikationssysteme in deren Visier geraten. Je konformer unsere Systeme sind, desto anfälliger.

**R**edundanz ist gut, aber sie muss durch Diversität ergänzt werden, sonst werden die weltweiten Informatiksysteme zur Achillesferse der entwickelten Volkswirtschaften. Die Abhängigkeit unserer Wirtschaft von den Informatiksystemen und Standards ist enorm. Wir arbeiten alle mit denselben Microsoft-Programmen und IP-Protokollen. Und genau das macht uns anfällig. Es gilt, mehr in die Diversität zu stecken, sonst haben Terroristen, die einen «e-Jihad» planen, ein leichtes Spiel. Keine Frage: Der massive Einsatz der Informationstechnologie hat die Finanzindustrie effizienter gemacht.

**BRIGITTE STREBEL**

Dank der Entwicklung und Einführung allgemein gültiger Standards wurde Routinearbeit rationalisiert und automatisiert. Das ist positiv. Aber es gibt einen weiteren Aspekt, der zum Nachdenken anregt: Je allgemein gültiger die Standards und IT-Architekturen, desto anfälliger und abhängiger werden ganze Volkswirtschaften rund um den Globus von diesen Systemen und ihrem reibungslosen Funktionieren. «Wir geraten jetzt langsam in eine Zone hinein, wo wir darauf achten müssen, nicht nur und ausschliesslich operationelle Monokulturen zu pflegen», mahnt Daniel Wettstein, der als Direktor der Schweizerischen Nationalbank für das operationelle Bankgeschäft verantwortlich zeichnet. Monokulturen seien immer problematisch und würden zu Abhängigkeiten und Anfälligkeiten führen, erklärt er und verweist in diesem Zusammenhang auf das Beispiel der Landwirtschaft, wo inzwischen bereits die Artenvielfalt bedroht ist. Ein weiteres Beispiel gebe die Antibiotika-Produktion in der Pharmaindustrie, wo sich inzwischen gefährliche Resistenzen eingestellt haben.

## Redundanz mit Diversität ergänzen

In der Finanzindustrie ist in der Vergangenheit sehr viel in die so genannten Kernsysteme und deren Redundanzen investiert worden. «Das ist eigentlich alles in Ordnung. Aber gerade der vergangene Jahrtausendwechsel hat uns drastisch gezeigt, was es für alle bedeutet, wenn sich irgendwo ein relativ kleiner Fehler einschleicht. Deshalb brauchen wir zusätzlich zur Redundanz auch Diversität in den Informatiksystemen», erklärt Wettstein. Gerade im Zahlungsverkehr sei dies äusserst wichtig. Vor kurzem habe er die Mitglieder der Kommission für Sicherheit im Zahlungsverkehr zur Besichtigung eines Kernkraftwerks eingeladen. «Hier geht es um Leib und Leben, deshalb ist man sich der Notwendigkeit einer Diversität bewusst, in dem zum Beispiel gewisse Installationen völlig unabhängig in Bezug auf Technik und Ablauf voneinander funktionieren.» Also geht es nicht nur um die Duplizierung der Systeme, sondern auch um deren völlig unterschiedliche Konstruktion und Prozessabläufe. Nur so kann man sich gegenüber dem Einschleusen von «Bugs»

oder Viren schützen. «Was nützen zwei- oder dreifach gleichzeitig geschaltete Systeme, wenn niemand mehr Zugriff zu ihnen hat?», gibt Wettstein zu bedenken. Bisher haben wir um unsere Systeme schöne Schutzhüllen gebaut. Aber was nützt das, wenn das Netzwerk zu diesen Systemen plötzlich nicht mehr funktioniert?»

Die neue Sicherheitsphilosophie fordert die Unternehmen mit neuen Budgetproblemen heraus, dessen ist sich Wettstein bewusst, der neben seiner Aufgabe bei der Nationalbank auch noch als Präsident von SWIFT Switzerland, National Member and User Group (NMUG), amtiert. Diversität ist zwar «nice to have», aber teuer. Die IT-Industrie wird dies freuen. Ernsthaft Sorgen bereitet ihm aber auch die Abhängigkeit der Finanzindustrie von den Telecom-Providern. «Weder wir noch die Industrie selbst wissen ganz genau, ob und wo die «single points of failure» zu finden sind. Hier ist sicher Handlungsbedarf angesagt.» Am besten sieht man dies auch bei weltweiten Standards, wie sie von Microsoft gesetzt worden sind. Diese leiden am heftigsten unter den immer häufiger werdenden E-Attacken. So hat es ein relativ simples Virus, wie Sasser, geschafft, in gewissen Regionen die Bancomaten ausser Funktion zu setzen. Sorgen bereitet Wettstein auch die Tatsache, dass viele Institute nicht mehr in der Lage sind, bezüglich Prävention gegen E-Attacken die richtigen Prioritäten bei Transaktionen zu setzen. «Eine Bet-



ty-Bossi-Zahlung kann auch noch übermorgen erfolgen, aber die weltweite Liquiditätsbeschaffung im Interbankengeschäft, Verbindungen zu Custodians und Money-Market-Transaktionen sind sehr zeitkritisch.» Das tragische Ereignis vom 11. September 2001 habe vielerorts das Bewusstsein für gewisse Massnahmen geschärft, meint Wettstein, dasselbe sollte jedoch auch im virtuellen Bereich erfolgen. Probleme in diesem Bereich können sehr leicht zu eigentlichen Reputationsrisiken nicht nur für einzelne Institute, sondern für den gesamten Finanzplatz ausarten.

### Business-Continuity-Projekt gestartet

Daniel Wettstein ist sozusagen der Wächter über das Swiss Interbank Clearing, den schweizerischen Zahlungsverkehr. Wie soll die Finanz- und insbesondere die Zahlungsverkehrsindustrie ihre Prioritäten setzen? Spontan nennt er drei Faktoren: Als Erstes geht es um die Entwicklung eines speziellen Netzwerks, das den Informationsaustausch und die lebenswichtige Koordination in einem solchen Krisenfall garantiert. Dieses Projekt ist bereits gestartet worden, indem eine entsprechende Arbeitsgruppe für das Business Continuity Program (BCP) von EBK, SNB, SBVg sowie Telekurs Group und den grossen Instituten etabliert worden ist. Hier sind die wichtigsten Player der Finanzwirtschaft auf den verschiedensten Ebenen involviert. Einzelne Krisenstäbe zum Beispiel im Rahmen des SIC habe es bereits früher gegeben, inzwischen gehe es aber darum, die Teilnehmer miteinander zu vernetzen, um so im Krisenfall ein rasches und effizientes Eingreifen zu ermöglichen. Die Kleinräumigkeit der Schweiz und das Verständnis zum vernetzten Handeln erleichtere ein solches Krisendispositiv, erklärt Wettstein. Zweitens möchte er über die Finanzwirtschaft hinaus auch andere Industriezweige, wie die Strom- und Telecom-Industrie, mit ins Krisendispositiv einbeziehen. So sollte eine Bank von einer gewissen Grösse an zwei verschiedene Telecom-Provider benutzen. Dabei dürfe man sich nicht auf das eigene Haus beschränken, sondern seine Sicht darüber hinaus ausweiten und Redundanzen und Diversitäten mit einzubeziehen. Eigentlich würde dies eine Art weltweites Parallel-Internet erfordern, um alle Eventualitäten abzudecken. Als Drittes müsse man nun bei Grossprojekten über die Bücher

**SNB-Direktor Daniel Wettstein: IT-Monokulturen machen abhängig und verwundbar.**

und prüfen, wie die ersten beiden Faktoren, das Netzwerk für Krisenfälle und der Einbezug anderer anfälliger Branchen, berücksichtigt werden können. Der Browser von Microsoft gehört inzwischen zu den weltweit besonders kritischen Systemen. Deshalb sei auch das totale Outsourcing von Software nicht so problemlos. Noch vor ein paar Jahren hatte Sun Microsystems Gründer Scott McNealy noch mit dem Ausspruch «The network is the computer» ein neues Zeitalter vorhergesagt. Bloss wurde zu jener Zeit das Thema Security nicht diskutiert.

«Wohlverstanden, wir können nicht für alles und jedes eine Lösung haben. Das wäre schlichtweg zu teuer», meint Wettstein. Für ihn ist klar, dass die Finanzindustrie diese Probleme aus eigener Kraft lösen muss. Er betont, dass sich seine Sicht auf den operativen Bereich konzentriere und nicht etwa auf den Finanzstabilitätsbereich. Das sei Sa-

## Die Kommunikation ist das zentrale Element

«Im Störfall – möglichst bevor es zur Krise kommt – ist die Kommunikation aller Verantwortlichen ein entscheidendes Element zur Meisterung der Situation. Der Finanzplatz Schweiz verfügt, wie andere Bereiche auch, traditionell über ein gutes Netzwerk der verantwortlichen Stellen. So besteht seit Jahren ein Krisenstab für das SIC/euroSIC-System mit Beteiligung der wichtigsten Finanzinstitute und der Provider (Telekurs) unter Leitung der SNB. Letztmals kam dieser Stab bei den Netzwerkstörungen vom 30. Juni live zum Einsatz. Unter Federführung der EBK/SNB hat jetzt eine Arbeitsgruppe BCP (Business Continuity Program) eine erweiterte Krisenorganisation etabliert. Diese Organisation befasst sich mit Problemen, welche den Finanzplatz insgesamt betreffen. Jede Institution ist innerhalb ihrer eigenen Organisation für die notwendigen Vorkehrungen selbst verantwortlich. Neu werden nicht nur die Belange des Interbank-Verkehrs (SIC/euroSIC), sondern auch des Retail-Verkehrs, die Liquiditätsversorgung und das oberste Management miteinbezogen. Die Verantwortlichen aller dieser Ebenen und Institutionen sind in einer Alarmorganisation zusammengefasst. Diese Personen schalten sich im Ausnahmefall rasch zusammen, tauschen Informationen aus, koordinieren geeignete Massnahmen und stellen die Kommunikation zur Öffentlichkeit sicher. Wichtigstes Element dieser Organisation ist die Kommunikation: ein Netz von Fachleuten, die sich kennen und einander vertrauen. Krisenhandbücher sind in diesem Bereich von sekundärer Bedeutung. Der geeignete Einbezug von weiteren für die Finanzindustrie wichtigen Partnern z. B. aus den Bereichen Telekom, Energie und Softwareanbietern ist in Bearbeitung. Hier muss noch Überzeugungs- und Aufbauarbeit geleistet werden», betont SNB Direktor Daniel Wettstein.

## Kritische Netzinfrastrukturen

Anbieter von kritischen Netzinfrastrukturen und Front-End-Lösungen mit einer hohen Marktdurchdringung wie Swisscom und Microsoft müssen vermehrt zu den folgenden Fragen Stellung beziehen:

- Bedeutung und Konsequenzen eines Ausfalls ihrer Lösungen für die Finanzindustrie und die Volkswirtschaft
- Vorkehrungen und Hilfestellungen im Falle eines Gaus
- Beteiligung am Krisen- und Business-Continuity-Program-Management in der Finanzindustrie
- Informationspolitik in Bezug auf eigene Produkte
- Problem von Monokulturen mit fehlender Diversität

che des von Niklaus Blattner angeführten Departements für Systemstabilität innerhalb der SNB. Dennoch, Basel II befasst sich implizit mit den operationellen Risiken, die jetzt immer greifbarer werden. Die Systemüberwacher der SNB würden diese Probleme von einer globaleren und übergeordneteren Sicht beurteilen, erklärt Wettstein. Er hingegen kümmert sich um den operativen Bereich und versteht sich eher als Feuerwehrmann in einem speziellen Team, das von den verschiedenen Providern wie Telekurs, SIS und den Rechenzentren unterstützt werde. Wettstein betont, dass die Schweiz mit keinen akuten Bedrohungsszenarien konfrontiert sei, aber es gelte, in gewisser Weise Vorsorge zu treffen, um potenziellen Exposures unseres Landes entgegenzuwirken. Letztlich bestimmt die Systemstabilität des Schweizer Finanzplatzes auch dessen Reputation. ■