

»Faktenreich, locker und präzise formuliert, mit leicht ironischem Unterton – Müllers Insiderreport liest sich wie ein Kriminalroman.« *Rheinischer Merkur*

An der Zürcher Bahnhofstraße wird ein Drittel des Weltprivatvermögens verwaltet. In seiner Reportage deckt Leo Müller die geheimen Geschäfte und Machenschaften prominenter Geldtouristen auf und erklärt, wie das System von der mächtigen Kundschaft geschützt wird. Beim Ausflug in die Welt des modernen Corporate Crime begegnet man nicht nur gewieften Gehilfen in Geldhäusern und Anwaltskanzleien mit ihren raffinierten Steuertricks, sondern auch machtlosen Strafverfolgern – und einigen bekannten Gestalten ...



Lüthy + Stocker AG Sihlcity

62010

BZ 2679 347 6168238 / 12.07.07

ULL 36949; Müller L: Tatort Zürich

Econ-Ullstein-List

92968

CHF inkl. MwSt 1-

16.90

62N



www.ullstein-taschenbuch.de

ullstein Leo Müller Tatort Zürich ullstein



Leo Müller Tatort Zürich

Einblicke in die Schattenwelt
der internationalen Finanzkriminalität

ullstein

fixiert sein. Aber wie sieht es dort in der Praxis aus? Halten sich die Behörden an diese Standards, so wie es Europäer gewohnt sind? Besteht der Bankengesetz-Artikel 47 aus dem Jahre 1934 den Praxistext im 21. Jahrhundert?

160 Megabyte Kundendaten in der Redaktionspost

Diese Fragen haben zahlreiche Kunden im Frühsommer 2005 mit ihren Rechtsberatern erörtert – aus einem für sie sehr unangenehmen Anlass: Erstmals war am Zürcher Bankenplatz der Geheimnis-Supergau eingetreten. Kundendaten waren der Zürcher Redaktion der größten Schweizer Wirtschaftszeitung anonym zugestellt worden. Betroffen waren ausgerechnet jene Klienten, die erhöhten Diskretionsschutz für ihre Milliardenvermögen suchten.

Die CD-ROM in der Redaktionspost enthielt kein Zeichen des Urhebers, keine Beschriftung, kein Signet – es war handelsübliche Massenware aus dem Computershop. Der Inhalt hingegen war absolut nicht für den allgemeinen Gebrauch bestimmt: 169 Megabyte umfassende Dateien mit Kunden- und Geschäftsdaten des größten Schweizer Vermögensverwalters, dessen Weltruf auf Verschwiegenheit aufbaute und der rund 270 Milliarden Franken Kundengelder betreut. Die Datensätze, das wurde schnell klar, stammten aus dem Büro der Julius-Bär-Gruppe auf den Cayman Islands. Sie wurden in den Jahren 1997 bis 2003 erstellt und betrafen große Teile des geschäftlichen Ablaufs der Bär-Firmen auf der Karibikinsel und eine Kundenklientel, die es gerne besonders vertraulich geregelt hat: sehr vermögende Privatkunden aus der ganzen Welt.

Es waren Kunden dies- und jenseits des Atlantiks, schwerreiche Erben, gestandene Unternehmerpersönlichkeiten, bekannte und weniger prominente Personen aus Politik, Wirtschaft und Kultur, auch wohlhabende Schweizer Bürger. Sie ließen sich von ihren

Anwälten oder direkt von der Julius Baer Bank and Trust Company und der Julius Baer Trust Company (Cayman) Stiftungen, Domizilgesellschaften und Trusts zur Verwaltung ihrer Vermögen einrichten.

Diese Firmen hatten in der Regel ihren Sitz in karibischen Inselstaaten oder auf den britischen Kanalinseln. Deren Konti wiederum befanden sich bei Julius Bär in New York oder Zürich, hin und wieder auch bei anderen Geldinstituten. Es waren die üblichen Konstruktionen, die superreiche Anleger wählen, um ihr weltweit verstreutes Vermögen zu verwalten.

Nachdem der Fall publik wurde, forschte das Bankhaus mit Hochdruck nach dem Datendieb. Die verdächtige Person hatte sogar Zugriff auf die Sitzungsprotokolle des Managements, verfügte über vertrauliche Besprechungsnotizen mit Fondsgesellschaften, konnte interne Gebührenberechnungen und nichtöffentliche Bilanzen einsehen.

Die Weitergabe von sensiblen Informationen ist ein Risiko, mit dem jedes Unternehmen leben muss, auch feinste Bankhäuser und verschwiegene Treuhänder: frustrierte Mitarbeiter, rachsüchtige Gekündigte, die Verlierer im Backoffice haben Motive genug. Bei der Bär-Bank glaubten die Männer von der Sicherheit, an alles gedacht zu haben. Bernhard Hodler, der Chief Risk Officer, und Giampaolo Trenta, der Chief Security Officer, hatten kurz zuvor in der gesamten Bankengruppe einen »Leitfaden für den sicheren Umgang mit Kunden- und Geschäftsdaten« verschickt. Ob in Zürich oder Basel, in Dubai oder New York – die Broschüre im CD-Hüllen-Format war Pflichtlektüre für jeden Mitarbeiter. Der verbindliche Leitfaden klärte über die praktischen Seiten des Bankkundengeheimnisses auf. Von Passwörtern und vom Virenschutz war die Rede, vom korrekten Zugangsschutz zu den Computern und vom sorgsamem Umgang mit dem Notebook. So dürfen Portfolio-Manager auf Auslandsreisen ihren Laptop nur mit verschlüsselter Festplatte mitführen. Die Experten von der Privatbank wussten, dass ihr Institut wie jedes andere Unternehmen durch den Einsatz moderner Datenbanken und IT-Technik

»verletzlich« geworden ist. Sie gaben den Mitarbeitern zu bedenken, dass Hacking und Datendiebstahl nicht nur zu finanziellen Schäden führen. Im Leitfaden stand ganz unmissverständlich: »Der damit oft einhergehende Reputationsverlust kann um ein Vielfaches größer und existenzgefährdend sein.«³

Kaum ein Kunde im Private Banking hat eine Vorstellung davon, in wie vielen Kontexten sein Name und Hinweise über seine Konti oder Anlagevehikel in den Geldhäusern gespeichert sind. Sensible Datenspuren sind gewöhnlich in Dutzenden von Textdateien zu finden. Zum Beispiel in gespeicherten Faxbriefen, die zwischen der Trustverwaltung und dem Portfolio-Manager versandt wurden. Oder in Dateien mit den Reglements der Trustfirmen sowie in Listen über Kredit- und Investment-Geschäfte. Kundenbetreuer und Vermögensverwalter legen wiederum Datenbank- und Tabellendateien an, in denen sie die Adressen von Kontoinhabern, Anwälten, Asset-Managern, Treuhändern und den »beneficial owners« notieren. Assistenten im Backoffice fertigen mit ihrem Textverarbeitungsprogramm Inventarblätter für die Kundensafes an. Eine Datenkopie bleibt auf der Festplatte gespeichert. So findet man dann zum Beispiel den Namen des Verfassers eines Testaments, das im Safe abgelegt wurde. Und Kundenbetreuer zeichnen bei komplexen, verschachtelten Anlagevehikeln Organigramme mit der Grafiksoftware – als Gedächtnisstütze. Die ganz normale Arbeit der Angestellten führt dazu, dass die Namen der Klienten dutzendfach im Rechnernetz vorhanden sind.⁴

Dieser Umstand wäre nicht weiter gefährlich, wenn die Daten nur wenigen Mitarbeitern zugänglich wären. Doch ohne Informationen können die Banker nicht arbeiten. Zudem verlangen gesetzliche Aufbewahrungspflichten, dass viele Kundeninformationen langfristig gespeichert werden. Besonders deutlich wird das Datenschutz-Dilemma am Alltagsproblem der Systemadministratoren: den Computerviren. Banker kommunizieren per E-Mail mit Fondsverwaltern, Vermögensmanagern, Kommunikationsfirmen und natürlich mit den Kollegen im Firmennetz. So können Viren, »Würmer« und »Trojaner« in die Netze eindringen, die Software

und die Daten schädigen, im schlimmsten Fall sogar elektronisch ausspionieren.

E-Mails können inzwischen verschlüsselt werden, auch Faxleitungen sind ein sicherer Kommunikationsweg. Aber die Datenbestände auf den Festplatten sind häufig nicht kryptiert. Denn sonst könnten Virenschutzprogramme die Dateien nicht auf schädlichen Befall absuchen. In gediegenen Prospekten ist das Bankkundengeheimnis schnell und ohne Wenn und Aber garantiert. Für deren tatsächliche Einhaltung müssen die Computerexperten sorgen. Der Bank Julius Bär blieb nur die verhaltene Krisenkommunikation: »Das Restrisiko ›Mitarbeiter‹ kann kein Unternehmen trotz modernster Infrastruktur und Sicherheitsmaßnahmen vollständig ausschließen. Deshalb versuchen wir mit einer sorgfältigen Rekrutierung unserer Mitarbeiter sowie laufender Prävention diese Gefahr zu minimieren. Zur Klärung des vorliegenden Falles arbeiten wir eng mit der Polizei und anderen Behörden zusammen.«

Die Bank erstattete Strafanzeige. Doch die Kunden, ob betroffen oder nicht, schickten ihre Anwälte los. Viele von ihnen hatten sich in den vergangenen Jahren über politische Angriffe auf das Bankgeheimnis Sorgen gemacht. Aber dass die Gefahr ausgerechnet bei diesem Institut, das für Tradition und Geschichte steht, von einer ungesicherten Harddisk ausging, ahnte wohl kaum ein Klient.

Ein Bankier redet Tacheles

Die Privatbank ist von der überragenden Persönlichkeit Hans J. Bär geprägt worden. Der 1927 geborene Grandseigneur des Zürcher Bankenplatzes war 1947 in das vom Großvater gegründete Institut eingetreten, verbrachte seine Lehrjahre in New York und baute zusammen mit seinen Cousins ein transatlantisches Beziehungsgeflecht zwischen Finanzbranche, Musikwelt und Ökonomie auf, das der Bank Kundenvermögen jenseits der Hundert-Milliarden-Grenze einbrachte. Die Schweizer Banken verdanken seiner diplomatisch-politischen Weitsicht die Lösung der bizarren

Diskussion um den Verbleib jüdischer Vermögen. Die öffentliche Debatte darüber, wo eigentlich das in der Schweiz angelegte Geld der im Holocaust ermordeten Juden geblieben war, hatte der Schweiz die schwerste Krise der Nachkriegszeit beschert. Mit Hilfe seiner exzellenten Kontakte ins amerikanische Establishment erreichte Hans J. Bär die Gründung einer Kommission unter der Leitung des ehemaligen US-Notenbank-Präsidenten Paul Volcker, die schließlich eine Vereinbarung über die Auszahlung der Vermögen an die Hinterbliebenen ermöglichte.

Als er im Jahr 2004 seine Memoiren vorlegte, ging ein Raunen durch die Bahnhofstrasse. Sie wurden zur Anklageschrift gegen das Räubertum in der Wirtschaft. »Recht hat er«, tuschelten die Rechtschaffenen. »Wenn er das nicht so direkt gesagt hätte!«, meinten die Furchtsamen. Bär hatte sich erlaubt, Tacheles zu schreiben. Sein Ethik-Kapitel überschrieb er mit einem abgewandelten Shakespeare-Bonmot der zynischen Figur Sir John Falstaff: »Merkt euch, ihr Stümper, man stiehlt beizeiten und mit Anmut«, und fügte hinzu: »Vielleicht wird gar nicht einmal soviel mehr gestohlen als früher, aber es fehlt einfach die Anmut.«⁵

Hans J. Bär ärgert sich über den »verschwenderischen Gebrauch« des Ethik-Begriffes. In Anlehnung an Max Webers berühmten Essay über »Politik als Beruf« urteilt Bär über die aktuelle Situation: »Heute erleben wir weder Gesinnung noch Verantwortung, dafür aber anstelle der Arbeitsethik eine neue Schöpfung: die ›Bereicherungsethik‹.« Als wirklichen Ehrenmann betrachtet Bär den italienischen Manager Raoul Gardini, der den Freitod wählte, als nach einem mutmaßlichen Betrug die Verhaftung drohte: »Neu ist höchstens, dass sich niemand mehr erschießt oder erhängt, wenn der Skandal ruchbar wird.« Die heutige CEO-Generation lasse eine »fehlende Kinderstube« erkennen.

Nicht alle »Bären« waren angetan davon, wie der Patron den Jungbankern die Leviten gelesen hatte. Im Jahr nach der Publikation seiner Memoiren wurde es im Hause Bär turbulent. Die modernen Zeiten brachen nun auch über sein Haus herein. Sohn Raymond setzte im Verwaltungsrat durch, dass die Familie das ge-

samte Kapital der Bank für das Börsenpublikum öffnete. Wachstum war das Ziel, eine »kritische Größe« an verwaltetem Kundenvermögen sollte erreicht werden, um die gestiegenen Kosten für die Geldwäschekontrollen in den Backoffices und die Akquisition neuer Kunden bezahlen zu können. Im September 2005 verkündete Raymond Bär, dass künftig Abgesandte der Giganten aus dem Hause des Finanzdienstleisters UBS von schräg gegenüber an der Bahnhofstrasse in die Chefetage einziehen würden. Der verkündete Deal war recht raffiniert: Julius Bär übernimmt aus dem UBS-Konzern drei kleine Privatbanken mit rund 119 Milliarden Franken Kundenvermögen, deren durchmischte Klientschaft nicht mehr in ein an der Wall Street kotiertes Unternehmen passte. Im Dezember 2006 wurden bei Julius Bär insgesamt Kundenvermögen von rund 360 Milliarden Franken betreut. Die bittere Pille dabei war, dass nun die UBS als Großaktionär im Haus sitzt und Schlüsselpositionen im Management besetzt.

Daten-Katastrophen und Datendiebe

Auch die UBS kennt das Thema »Daten-Desaster« im Betriebsalltag. Anfang Juni 2005 meldete die Niederlassung in Tokio einen Festplattenverlust. Die Großbank gab eine beschwichtigende Notiz an die Medien: »Das Risiko, dass Kundendaten in unbefugte Hände gelangen, ist gering, da die Daten in einem speziellen Format gespeichert wurden und nur schwer zugänglich sind.« Von den Konzernverantwortlichen wurde der Vorfall freilich nicht auf die leichte Schulter genommen: Die Aufsichtsbehörden wurden davon ebenso informiert wie die betroffenen Kunden. Einige Tage später berichtete die amerikanische Citigroup, dass in der Frachtpost Datenträger mit vier Millionen Kundennamen verschwunden sind. Ein Datenverlust bei der Bank of America betrifft 1,2 Millionen Kunden.

Datendiebstahl ist ein Wachstumsgeschäft. In den USA raubten Kriminelle Kundendaten der Auskunftsfirma Choicepoint, um