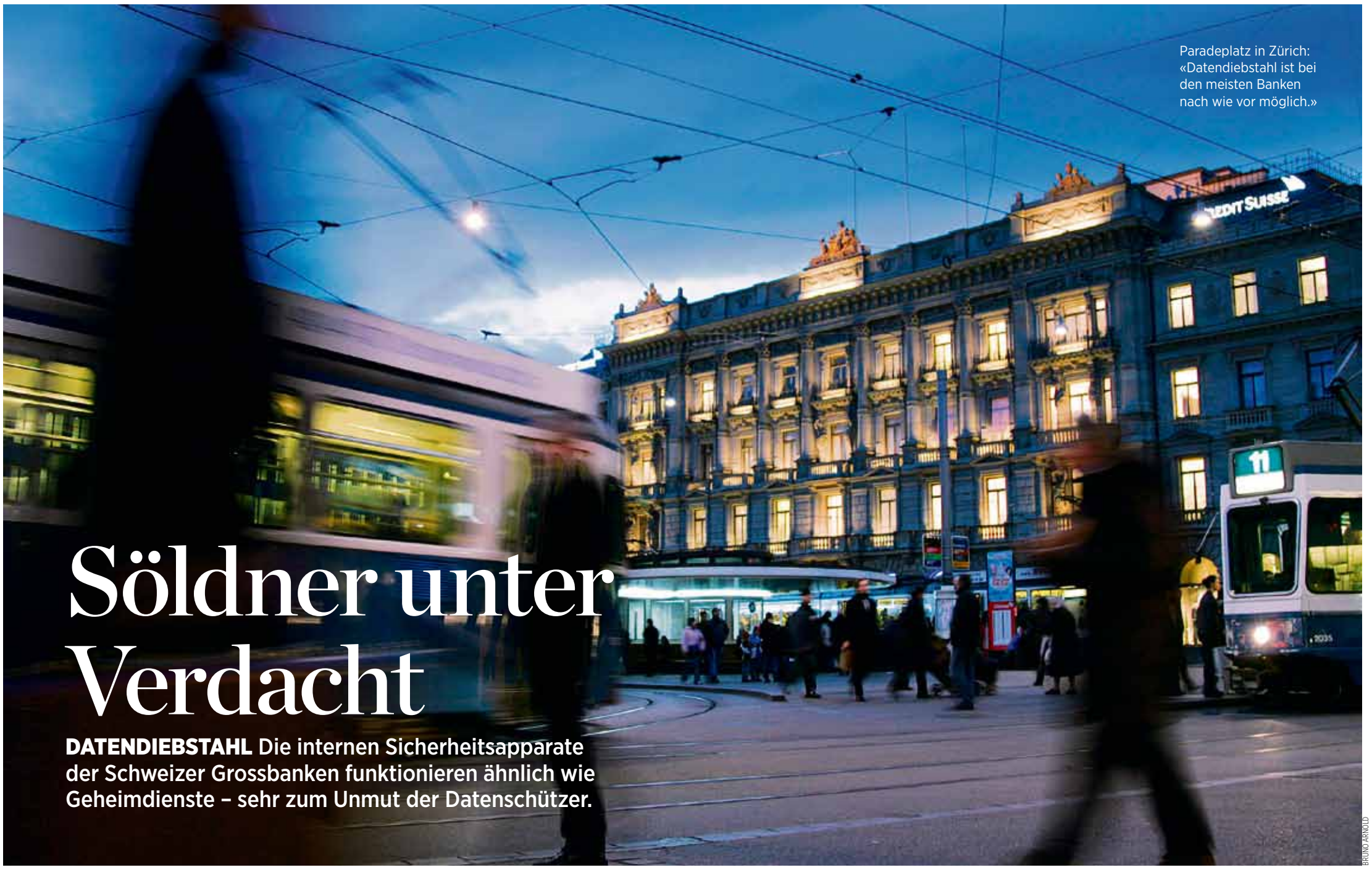
Finanz

Höhenangst
Trotz grosser Ungleichgewichte kaufen die Anleger weiter zu. Das erhöht die Absturzgefahr. **Seite 25**

Temporausch
Der Schnellhandel an den Börsen soll begrenzt werden. Das birgt neue Gefahren. **Seite 22**



Paradeplatz in Zürich: «Datendiebstahl ist bei den meisten Banken nach wie vor möglich.»

BRUNO ARNOLD

Söldner unter Verdacht

DATENDIEBSTAHL Die internen Sicherheitsapparate der Schweizer Grossbanken funktionieren ähnlich wie Geheimdienste – sehr zum Unmut der Datenschützer.

BERNHARD FISCHER, GÉRARD MOINAT

Michael Alkalay weiss, wie der typische Bankdatendieb tickt. «Zumeist Vermögensberater, von Frau und Kind verlassen, frustriert und zudem hoch verschuldet», beschreibt der Kriminalist und Luzerner Hochschulprofessor das Profil. Der Chef des Bankers sei bereits der vierte in fünf Jahren. Es würden nur Margen, Gebühren und Boni zählen. «Die Mitarbeiter kümmern sich dann nicht mehr um Anstand, das wird ihnen von der Führung auch vorgelebt», sagt Alkalay. Man gehe dorthin, wo am meisten bezahlt wird. Bankmitarbeiter verhielten sich heutzutage «wie Söldner».

Hacker wechseln die Seite

Von deutschen Steuerfahndern lassen sie sich inzwischen fast regelmässig bezahlen. Das Geschäft der Datendiebe floriert. Für die CDs mit den gestohlenen Kontodaten blättern die Staatsdiener Millionen auf den Tisch, wie wohl jüngst wieder in Nordrhein-Westfalen. Der dortige Finanzminister Norbert Walter-Borjans soll grünes Licht für den Ankauf eines Datenträgers mit Informationen zu Kunden der UBS gegeben haben. Die Bank will jedoch von einem Datenleck nichts wissen.

Noch weiss keiner, wie viele CDs von welchen Banken derzeit im Umlauf sind. Doch auch die jüngste Welle im undurchsichtigen Handel mit Bankdaten erschüttert die Hochfinanz. Im Gegenzug eröffnet sie die Jagd auf potenzielle Datendiebe. Entsprechend hektisch rüsten vor allem die Grossbanken ihre internen Sicherheitsabteilungen auf und verschärfen die Überwachung ihrer Mitarbeiter.

Im jüngsten Fall des mutmasslichen Datenklaus laufen bei der UBS alle Fäden in der Abteilung der Group Internal Audit (GIA) zusammen – auch als interne Revision bekannt und gefürchtet. Dort sitzt unter anderem der hauseigene Geheimdienst des Finanzgiganten. Die Experten verfolgen Datenspuren und werten Kameraaufnahmen im Rahmen des Objektschutzes aus. «Ich wurde schon über meine Datenzugriffe befragt und zur Rechenschaft gezogen», erzählt ein UBS-Mitarbeiter. Notizen von Kundentreffen, Aufzeichnungen auf Karteikarten und systeminterne elektronische Einträge wurden durchforstet.

Die Hauptwaffe der Bankpolizisten ist jedoch die Überwachung des Mailverkehrs mit Hilfe elektronischer Filter. Kommen bestimmte Stichwörter vor, die auffällig sind oder in einem spezifischen Arbeitskontext nicht vorkommen sollten, dann schlägt das System Alarm. Ein begründeter Verdacht genügt, um die Mails der Mitarbeiter auch unbemerkt und über einen längeren Zeitraum zu überwachen. Mehr Details will der UBS-Insider nicht preisgeben. Die Begründung erinnert an die Zeiten des Kalten Krieges. «Man will der Gegenseite keine Munition liefern.»

Seine Kollegen von der Credit Suisse geben sich ähnlich zugeknöpft. Aber auch sie leisten sich teuerste Überwachungstechnik. Unter dem Codenamen «Ratoc» fliessen seit vorletztem Jahr Millionen in ein Grossprojekt zur Sicherung der Kundendaten. (HZ 18.8.2011) Totale Mailüberwachung und harte Verhöre mit Verdächtigten sind dabei Routine. Oberster Sicherheitschef der CS ist Heinz Leibundgut. Mit fast 300 Mitarbeitern durchleuchtet er die «Risiken der einzelnen Geschäftstätigkeiten».

Totale Mailüberwachung und harte Verhöre sind Routine.

Der Mann, welcher die internen Überwachungssysteme der UBS koordiniert, heisst James P. Oates. Er ist der Chef des GIA und beschäftigt mehr als 300 Mitarbeiter. Sie haben uneingeschränkten Zugang zu allen Daten, Geschäftsbüchern, Dokumenten, Systemen, Räumlichkeiten und Mitarbeitern. Die Untersuchungsabteilung für kriminelle Angelegenheiten ist von der Compliance-Abteilung getrennt. Es gibt einen Compliance-Bereich, der ausschliesslich die Einhaltung der Regeln im grenzüberschreitenden Geschäft prüft. «Für jede Thematik gibt es Spezialisten» sagt ein UBS-Sprecher. Bewachungsdienst und Datenforensiker bilden wieder eigene Einheiten. «Die IT-Profis verfügen über die Fähigkeiten von Hackern, nur arbeiten sie für die Sache und nicht dagegen.»

Die UBS lässt sich diesen Aufwand etwas kosten. «Mehr als 100 Millionen Franken werden üblicherweise in einen Sicherheitsapparat dieser Grössenordnung für den Hauptsitz einer Bank gesteckt», sagt ein Sicherheitsarchitekt von Omnisec. Die Firma stattet nicht nur die Schweizer Grossbanken mit Sicherheitssystemen aus, sondern auch das Militär, Botschaften und Regierungen.

Heikel ist die hochtechnologische Mitarbeiterüberwachung allemal. «Bereits die Systemüberprüfung mittels Logfiles ist ein erheblicher Eingriff», sagt Francis Meier vom Eidgenössischen Datenschutz. «Würden Mitarbeiter nun zusätzlich per Kamera überwacht, wäre das ein massiver Eingriff in die Privatsphäre.» Bevor Überwachungskameras zum Einsatz kommen, müssen mildere Massnahmen eingesetzt werden wie etwas das Wegschliessen ihrer mobilen Geräte. Das Verhalten der Mitarbeiter am Arbeitsplatz zu überwachen, sei im Grunde gesetzlich verboten. Sollte es dennoch erforderlich sein, um Datendiebstahl zu verhindern, «dann dürfen die Massnahmen die Mitarbeiter in ihrer Gesundheit und Bewegungsfreiheit nicht beeinträchtigen», sagt Meier.

Ein Ex-Wirtschaftsermittler der Zürcher Polizei erzählt, was hinter den Kulissen abläuft. Von der Einzeltätertheorie geht die Polizei selten aus. Deshalb befragen die Privatfahnder auch das nächste Umfeld des betreffenden Mitarbeiters. Das sind Vorgesetzte und Kollegen. Bei einem begründeten Verdacht werden in der Regel Videoüberwachung, Observation und Telefonüberwachung eingesetzt. «In Fällen, wo Verdacht auf gesetzeswidriges Verhalten besteht, erstatten wir Strafanzeige und arbeiten eng mit den Untersuchungsbehörden zusammen», sagt ein UBS-Sprecher.

Die gemeinsame Abklärung ist notwendig, so der Ex-Polizist, «denn bei derartigen Ermittlungen stellen Verdunkelungsgefahr, Beweismittelvernichtung und die Beeinflussung von Informanten ein grosses Risiko dar». Mit dem Datenschutz würden es die Sicherheitsdienste der Banken dabei selten genau nehmen.

Die Kamera im Kugelschreiber

Im aktuellen Steuer-CD-Fall tappt die Grossbank noch im Dunkeln. Kein Tathergang wird ausgeschlossen. Mit hochauflösenden Kameras etwa, eingebaut im Kugelschreiber, können Mitarbeiter die Kundendaten nach wie vor vom Bildschirm fotografieren. «Auf dieser Ebene herrscht das Problem, dass immer mehr ihre privaten Geräte und Gadgets mitbringen wollen», sagt Sicherheitsexperte Erik Niklaus von Omnisec. Das Abspeichern auf USB-Sticks funktioniert nicht mehr. Dazu sind die Sicherheitsvorkehrungen mittlerweile zu streng. Hat ein Mitarbeiter der IT-Abteilung die Daten entwendet, kann er allenfalls eine externe Festplatte an den Server angeschlossen haben, um die Daten abzusaugen und auf eine CD zu brennen. Bei den vermögenden Kunden kommt die Schwierigkeit hinzu, dass die Kontodaten oft nur unter einem Code-Namen abgespeichert werden. Die wahren Namen der Kunden finden sich in einem Karteikartensystem, das abends weggesperrt wird.

Für Marc Ruef, Mitinhaber der Informatik-Sicherheitsberatungsfirma scip, ist klar: «Die Banken zahlen nun die Zeche dafür, dass sie seit vielen Jahren bestehende Sicherheitsprozesse nicht den aktuellen Gegebenheiten angepasst haben.» Beispiele für ungenügende Sicherheitsvorkehrungen finden sich etwa bei den Zugriffsrechten der Bankmitarbeiter. Diese sollten möglichst punktuell und restriktiv sein. Die Banken scheuen aber oft den administrativen Aufwand dafür. «Datendiebstahl ist bei den meisten Banken nach wie vor möglich», meint Ruef.

Damit das nicht mehr passiert, hilft laut Kriminalist Alkalay nur eines: «Der Chef muss sich wieder um seine Mitarbeiter kümmern. Nur wenn Loyalität und Integrität wieder mehr wert sind als das schnelle Geld, lässt sich der Datendiebstahl verhindern.»

SCHWEIZER BANKEN

Die schwersten Fälle von Datenklau

Julius Bär Rudolf Elmer, bis 2002 Geschäftsleiter der Julius Bär auf den Cayman Islands, versorgt nach seinem Abgang Medien, Steuerbehörden und die Enthüllungsplattform Wikileaks mit Kundendaten.

LGT 2006 verkauft der Angestellte der Liechtenstein Global Trust LGT Heinrich Kieber den deutschen Behörden Steuersünder-Informationen.

HSBC Der französische Informatiker Hervé Falciani der Genfer HSBC Private Bank verkauft 2008 gestohlene Kundendaten an Steuerbehörden.

Credit Suisse/Julius Bär Ein CS-Angestellter verkauft 2010 Kundendaten nach Deutschland. Die Staatsanwaltschaft Düsseldorf durchsucht CS-Filialen. Im Sommer 2010 erhält Nordrhein-Westfalen nach eigenen Angaben eine CD der Julius Bär.

Sarasin Ende 2011 versorgt ein Sarasin-IT-Mitarbeiter den SVP-Kantonsrat Hermann Lei nach dessen Angaben mit Details über Devisengeschäfte der Familie Hildebrand.

Coutts Im Juli 2012 sollen die nordrhein-westfälischen Behörden einen Datenträger gekauft haben. Betroffen sei die Zürcher Filiale der britischen Traditionsbank Coutts.

UBS Eine angeblich von nordrhein-westfälischen Steuerfahndern gekaufte Bankdaten-CD soll beweisen, dass die UBS deutschen Steuerpflichtigen hilft, ihre Vermögen aus der Schweiz nach Singapur zu transferieren. Die UBS dementiert.