Lecks und Leichtsinn

Informationssicherheit Die Finma verpflichtet Banken, sich besser gegen Datendiebe zu schützen. Experten fordern allerdings noch strengere Massnahmen.

BRUNO ARNOLD

Finanzmarktaufsicht: «Stossrichtung für einen wirkungsvolleren Schutz von elektronischen Kundendaten.»

OLIVIA KÜHNI

Der Informatiker L.O. fällt im Oktober 2011 einen folgenschweren Entscheid. Wie immer fährt der 54-jährige Deutsche von seinem Aargauer Wohnsitz aus in sein Büro bei der Bank Julius Bär. Doch statt sich um die Wartung der Computer zu kümmern, kopiert O. Kundendaten, speichert sie in Zip-Dateien und sendet diese an seine private E-Mail-Adresse. 15 Memos versandte O. auf diese Weise – von seiner Geschäftsadresse. Trotzdem flog er monatelang nicht auf.

Der Fall ist typisch. Wenn Kundendaten in den vergangenen Jahren eine Schweizer Bank verliessen, geschah dies fast immer auf dem Weg über E-Mail. Ein Leck, das in manchen Fällen zu verhindern gewesen wäre, hätten die Unternehmen entsprechende Sicherheitsmassnahmen installiert.

Jetzt zieht die Finanzmarktaufsicht Finma die Notbremse. Nach den wiederholten Datendiebstählen legt sie in einem Rundschreiben fest, wie Banken ihre elektronischen Kundendaten zu behandeln haben. Die Vorschriften, zu denen in den vergangenen Wochen Branchenvertreter angehört wurden, machen klar: Die Datensicherheit liegt in der Verantwortlichkeit des Top-Managements. Sicherheitsexperten begrüssen diesen Schritt. Sie hoffen, dass dies die Basis ist für weitere Schritte – etwa, dass Unternehmen irgendwann büssen müssen, wenn sie fahrlässig Daten verlieren.

Ganz ruhig Datensätze kopiert

Sicherheitsverantwortliche bei Banken berichten, dass die Datensicherheit bei manchen Instituten lange Zeit vernachlässigt worden ist. «Das Management liess ein paar Programme installieren, damit ihm niemand einen Vorwurf machen konnte, und damit hatte es sich», sagt der Compliance-Experte einer Bank. In der Regel würden Datenströme zwar gefiltert und verdächtige E-Mails gesammelt. Ausgewertet würden sie jedoch oft erst viel später.

So wie im Fall Bär, wo das von Informatiker O. geschlagene Leck erst auffiel, als der mutmassliche Täter bereits Datensätze von 2700 Kunden gesammelt und sie sich als Mailanhänge nach Hause geschickt hatte. Auch im Datenklau-Fall der Genfer HSBC kopierte der Dieb, ebenfalls ein Informatiker, über Monate hinweg unbemerkt Tausende von Datensätzen aus dem System. Bei der Credit Suisse wiederum reiste ein Kadermitarbeiter mit umfangreichen Adresssätzen auf dem Laptop nach Deutschland. Bemerkt wurde das erst, als deutsche Ermittler bei einer Razzia in der Frankfurter Filiale der CS auf den Laptop mitsamt Datenschatz stiessen und die Kunden angingen.

In London zahlte HSBC wegen Datenverlusten 3 Millionen Pfund Busse.

Nun verpflichtet die Finma alle Banken, die Datensicherheit zur Chefsache zu erklären. «Risiken im Zusammenhang mit der Vertraulichkeit von Kundendaten werden systematisch identifiziert, begrenzt und überwacht», heisst es im ersten Grundsatz ihres Rundschreibens. «Dazu überwacht der Verwaltungsrat die Geschäftsführung.» Diese wieder müsse eine Kontrollfunktion schaffen. Die Verantwortlichkeiten müssten klar und vom Verwaltungsrat abgesegnet sein.

«Es ist gut, dass die Finma dem Thema jetzt diese Priorität beimisst», sagt Thomas Koch. Der Sicherheitsexperte berät bei PwC Kunden aus der Finanzbranche. «Wir haben lange auf diesen Schritt gedrängt.» Dass die Finma den Umgang mit elektronischen Kundendaten erst jetzt aufnimmt, liegt in ihrem Selbstverständnis begründet.

Die Schweizer Aufsicht greift traditionell erst dann in den Markt ein, wenn die Beaufsichtigten wiederholt ins Unglück stolpern und selbst dann noch nicht dazulernen. Erst wenn die Eigenverantwortung der Banken offensichtlich nicht greift, werden die Finma-Experten aktiv. Selbstverständlich drückt der Sprecher der Aufsichtsbehörde dies anders aus. «Grundsätzlich handelt es sich bei Kundendaten um ein Thema, bei dem die Banken ein grosses Eigeninteresse an bestmöglicher Sicherheit haben sollten», sagt Tobias Lux. «Fälle aus der Vergangenheit haben gezeigt, dass nicht alle Institute ausreichende Massnahmen und Investitionen in diesem Bereich getätigt haben.» Entsprechend habe die Finma nun im Rundschreiben «die Stossrichtung für einen wirkungsvolleren Schutz von elektronischen Kundendaten umrissen».

Grundsätzlich sei es richtig, auf die Eigenverantwortung der Marktteilnehmer zu setzen, finden Compliance-Experten. Doch was die Finma vergesse, seien die internen Machtkämpfe. «Für die Bankspitzen ist Sicherheit in erster Linie ein Kostentreiber», heisst es. «Es braucht diesen Befehl aus Bern, damit sie diese Ausgabe vor den Eigentümern rechtfertigen wollen und können.» Compliance-Experten, die nicht namentlich genannt werden wollen, hoffen, dass die Schweiz noch weitergeht. Die Finma müsse Bussen aussprechen dürfen, wenn ein Unternehmen fahrlässig Kundendaten verliere. «Damit würde das Sicherheitsrisiko endlich zu einer harten Zahl», sagt einer von ihnen. Diese Haltung teilen viele Sicherheitsexperten. Sie wollen sich jedoch nicht öffentlich äussern, weil ihre Chefs eine Bussenkompetenz der Finma ablehnen. Dies fordert hingegen schon seit Jahren Monika Roth, Compliance-Expertin und Dozentin an der Hochschule für Wirtschaft in Luzern. «Ich vertrete seit längerem die Ansicht, dass die Finma die Kompetenz haben müsste, Bussen zu verhängen», sagte Roth im Dezember auf Radio SRF 1. Damals war bekannt geworden, dass die UBS in den USA eine Busse von 1,2 Milliarden Franken wegen Libor-Manipulationen ihrer Mitarbeiter zahlen muss. An die Finma gingen bescheidene 59 Millionen Franken an Gewinnrückgaben. Bussen verhängen können in der Schweiz nur die Wettbewerbskommission bei Marktabsprachen sowie das Finanzdepartement bei einem Verstoss gegen börsliche Meldepflichten.

Öffentliche Rüge statt Busse

Wenn die Finma künftig einen fahrlässigen Umgang mit Kundendaten feststellt, arbeitet sie also sanft wie immer: Mit den Mitteln des Dialogs, der Verfügung und der Rüge. In den vergangenen Jahren hat sie ausserdem begonnen, in besonders drastischen Fällen die Ergebnisse ihrer Untersuchungen öffentlich zu machen. So vermeldete sie im Februar 2011, dass sie bei HSBC nach dem Datendiebstahl «Mängel bei der internen Organisation und der Kontrolle der IT-Aktivitäten der Bank» gerügt habe. «Die Finma verlangt, dass HSBC den eingeschlagenen Weg fortsetzt und die Massnahmen zur Herstellung der erforderlichen IT-Sicherheit konsequent weiterführt», hiess es in der öffentlichen Mitteilung. Für das genannte Unternehmen kommt das einer Ohrfeige gleich – viel Schmerz, aber keine unmittelbar sichtbaren Kosten.

In Grossbritannien ist der Umgang mit den beaufsichtigten Banken und Versicherungen hingegen schärfer. Seit Jahren und wiederholt verhängt die britische Finanzaufsichtsbehörde Geldstrafen, wenn in einem Unternehmen wegen ungenügender Kontrollsysteme Kundendaten verloren gehen. Dies geschieht sogar, wenn nach einem Datenleck kein Kunde direkt zu Schaden kommt. Für eine Busse reicht es aus, dass ein Unternehmen die Kundendaten ungenügend schützte.

Ausgerechnet HSBC zahlte in Grossbritannien 2009 eine Geldstrafe von 3 Millionen Pfund für Organisationsmängel dreier Tochterunternehmen. Wegen «schwacher Kontrollsysteme» waren dort unverschlüsselte Kundendaten auf Datenträgern transportiert worden und teilweise verschwunden. Der Hypothekenfinanzierer Nationwide zahlte 2007 eine Busse von 980000 Pfund. Ein Mitarbeiter hatte einen Laptop mit Kundendaten mit nach Hause genommen, was niemand bemerkte. Dann wurde das Gerät gestohlen. Auch hier strafte die Aufsichtsbehörde, obwohl den Kunden nichts passierte. «Nationwide hat es versäumt, das Herunterladen von grossen Datenmengen auf portable Geräte zu überwachen», schrieb die FSA in ihrer Begründung. «Das bedeutet, dass das Unternehmen eine begrenzte Kontrolle über seine Daten und deren Nutzung hatte.»

Bei Julius Bär hätten die Erkenntnisse aus dem Fall O. «zu neuen Sicherheitsmassnahmen geführt», wie ein Sprecher sagt. Welche das sind, führte er nicht aus. Informatiker O. steht im August in Bellinzona vor dem Bundesstrafgericht. Weil er die Daten an einen pensionierten deutschen Steuerbeamten verkauft haben soll, muss er sich wegen wirtschaftlichen Nachrichtendienstes verantworten.

FINMA-RUNDSCHREIBEN

Neun Grundsätze zum Umgang mit Kundendaten

Risikopapier Die neuen Vorschriften hält die Finma in einem Rundschreiben mit dem Titel «Operationelle Risiken» fest. Sie widmet sich darin dem Umgang mit Geschäftsrisiken, etwa mit potenziellen Krisen.

Kundendaten Zum Umgang mit elektronischen Kundendaten hält die Finma neun Grundsätze fest.

1. Governance: Die Finma macht Informationssicherheit zur Chefsache. Der Verwaltungsrat überwacht die Geschäftsführung, die «Massnahmen zur Gewährleistung der Vertraulichkeit von Kundendaten» einsetzt. Die Geschäftsführung schafft eine unabhängige Kontrollfunktion.

2. Kundenidentifikationsdaten (Client Identifying Data): Die Banken müssen Kundendaten nach verschiedenen Vertraulichkeitsstufen kategorisieren. Das ist die Basis, um etwa unterschiedliche Zugriffsrechte festzulegen.

3. Datenspeicherung: Die Bank muss genau wissen, wo ihre Daten lagern und wer darauf zugreifen kann. Bei einer Speicherung im Ausland braucht es besonderen Schutz, etwa Verschlüsselung.

4. Technologie: Die Banken müssen technische Möglichkeiten nutzen, um die Sicherheit der Daten auf Geräten (insbesondere Mobilgeräten), auf Servern, sowie bei der Übertragung in Netzwerken sicherzustellen. Das können Sperren oder Verschlüsselung sein.

5. Mitarbeiter: Sie sind sorgfältig auszuwählen, auch wenn Externe beigezogen werden, und zu schulen. Die Bank verfügt über Listen mit den Namen jener Personen, die Zugriff auf Daten haben.

6. Risikokontrolle: Zuständig ist die erwähnte unabhängige Einheit.

7. Risikominderung: Vorsichtiges Verhalten, etwa Vieraugenprinzip und Meldungen bei Verdachtsfällen, einführen.

8. Kommunikation: Es muss klar sein, wie Vorfälle intern (Risikoabteilung, Management) sowie extern (Finma, Strafverfolgung, Medien) gemeldet werden.

9. Outsourcing: Die Verantwortung für die Daten bleibt bei der Bank. Sie muss die Standards des Partners nach klaren Kriterien regelmässig beurteilen.