

Der «Faktor Mensch» in der Bank

Trotz Vorkehrungen sind die Finanzhäuser gegen Datenmissbrauch nie ganz gefeit

Der Missbrauch von Bankdaten des gestrauchelten SNB-Präsidenten Philipp Hildebrand wirft ein Schlaglicht auf die Sicherheitssysteme bei Banken. Experten erwarten einen Aufschwung des Nummernkontos.

Michael Ferber

Der Rücktritt von Philipp Hildebrand als Präsident der Schweizerischen Nationalbank (SNB) rückt die Sicherheitsvorkehrungen von Banken gegenüber Datendiebstählen in den Blickpunkt. Wie schützen sich die Finanzhäuser vor Indiskretionen und Datenmissbräuchen durch eigene Mitarbeiter, wie sie im Fall Hildebrand bei der Bank Sarasin geschehen sind? Die Institute beteuern, sie verbessern laufend ihre Massnahmen. Ausschliessen lässt sich solcher Missbrauch aber nicht.

Wohl hohe Dunkelziffer

Laut einer Sprecherin der Schweizerischen Bankiervereinigung (SBVg) sind Banken gegenüber gut geplanten und mit krimineller Energie ausgeführten Datendiebstählen oft machtlos. Da helfe auch kein «Hochrüsten» bei den Sicherheitsvorkehrungen. Der «Faktor Mensch» lasse sich eben nicht einfach ausschalten. Wenn ein böswilliger oder gar eingeschleuster Mitarbeiter sich interne Bankdaten beschaffen wolle, werde es schwierig, diese vor ihm zu verbergen, sagt auch Hannes Lubich, Professor an der Fachhochschule Nordwestschweiz und IT-Sicherheitsexperte.

Ob die Zahl an solchen Delikten in den vergangenen Jahren zugenommen hat oder nicht, lässt sich naturgemäss nicht sagen. Schliesslich haben die Finanzhäuser überhaupt kein Interesse daran, dass solche Vorkommnisse an die Öffentlichkeit gelangen. Folglich lösen sie sie intern und machen sie gar nicht erst publik. Lubich geht davon aus, dass die Dunkelziffer in diesem Bereich sehr

hoch ist. Bei praktisch jeder Bank dürfte es solche Vorkommnisse geben.

Als beste Vorkehrungen gegenüber Missbräuchen gelten eine sorgfältige Rekrutierung von Personal und Schulungen. Besonders wichtig ist dies bei «Super Usern». Das sind Experten, die beispielsweise ein IT-System instand setzen sollen. Um ihre Aufgabe effizient erfüllen zu können, benötigen sie meist weitreichende Zugriffsrechte. Typischerweise wird dann laut Experten die interne Revision der Bank beauftragt, Mitarbeiter mit solch weitreichenden Kompetenzen temporär stärker zu überwachen. Aber nur mit einem extrem restriktiven System lassen sich Sicherheitslücken weitgehend schliessen. Dies ist nicht nur sehr teuer – es wird auch schwierig, überhaupt noch IT-Mitarbeiter zu finden, die unter solchen Bedingungen zu arbeiten bereit sind.

Laut der SBVg-Sprecherin sollten Bankdaten grundsätzlich nur für die Mitarbeiter freigeschaltet sein, die tatsächlich damit arbeiten müssen. Ausserdem sollten Mitarbeitende bankintern Ansprechpartner haben, die im Bereich Compliance tätig sind und an die sie sich bei Beobachtungen und im Verdachtsfall wenden könnten. Das Problem möglicher Datenmissbräuche lässt sich also nicht mit Technik allein lösen.

Eine weitere Vorkehrung ist die Verschlüsselung der Namen von Kunden, um deren Anonymität so weitgehend wie möglich zu wahren. Laut Lubich gibt es in Banken zumeist verschiedene IT-Systeme für unterschiedliche Aufgaben. Dabei müsse der Name des wirtschaftlich Berechtigten eines Kontos nicht stets in jedem System sichtbar oder auch nur vorhanden sein. Es sei aber schwierig, diesen Schutzmechanismus im Nachhinein einzuführen, wenn die Systeme ursprünglich nicht dafür entworfen und implementiert seien.

Cécile Aschwanden, Partnerin bei der IT-Beratungsgesellschaft Itopia, erwartet, dass die technischen Hürden in den Banken nach dem Fall Hildebrand heraufgesetzt werden. Ausserdem dürfe aus ihrer Sicht das Nummernkonto

wieder einen Aufschwung erleben. Hier ist der Kundename durch eine Nummer oder ein Wort ersetzt. Die Beraterin geht davon aus, dass der Fall Hildebrand nicht passiert wäre, wenn dieser ein solches Konto gehabt hätte. Nummernkonten gelten auch dann als vorteilhaft, wenn Dienstleistungen von Finanzinstituten in andere Länder outsourct werden.

Sauberer-Schreibtisch-Politik

Laut Lubich haben grosse Banken im Allgemeinen komplexere IT-Systeme als kleinere und sind beim Schutz ihrer Kundendaten mehr gefordert. Allerdings könnten sie nach seiner Meinung auch mehr Aufwand für ihre Verteidigung bezahlen. Kleinere Finanzhäuser und Privatbanken hingegen hätten hierfür wohl weniger Geld zur Verfügung, allerdings komme die soziale Kontrolle innerhalb einer kleineren Personalbasis stärker zum Tragen.

Die Grossbank UBS teilte auf Anfrage mit, sie habe klare Datenschutzrichtlinien und sehr hohe Sicherheitsstandards, die laufend überprüft und angepasst würden. Nur jene Mitarbeitenden hätten Zugang zu Daten, die diese für die Erfüllung ihrer Aufgaben benötigten. Laut Experten haben die meisten Banken auch Computer-Software installiert, die bei Wörtern wie beispielsweise «internal memo» in Mitarbeiter-Mails reagiert und IT-Sicherheits-Mitarbeiter darüber informiert. Dies geschieht auch, wenn in den Mails die Namen bestimmter Kunden erwähnt sind. Laut Bankenvertretern ist die Verschlüsselung von Kundennamen gängig, und in den Instituten gelte eine «Sauberer-Schreibtisch-Politik». Dabei werde auch überprüft, ob Mitarbeiter interne und geheime Dokumente weggeschlossen hätten.

Gegenüber dem Abfotografieren von Daten ab dem Bildschirm dürften die Banken hingegen weitgehend machtlos bleiben. Schliesslich gibt es nicht zuletzt auch Kameras, mit denen sich heimlich fotografieren lässt.